Introduction to Cyber Security

مقدمة للأمن السيبراني

دورة مجانية مقدمة من Cisco

المستوى: مبدئ

عندما كنت طفلاً، هل تخيلت نفسك كمدافع عن الكون يمتلك مهارات مذهلة - تدرك التهديد، وتحمي الأبرياء، وتبحث عن الأشرار، وتقدمهم إلى العدالة؟

هل تعلم أنك تستطيع أن تحصل على مهنة من ذلك؟

خبير الأمن السيبراني

الخبير الشرعي للأمن السيبراني

خبير أمن المعلومات

قرصان أخلاقي

كل هذه الأدوار يمكن أن تكون جزءًا من عملك في مجال الأمن السيبراني المثير والمتغير باستمرار.

تشتمل صفحة "دعم الطلاب" رابطًا إلى صفحة NetAcad Facebook وصفحتنا على موقع LinkedIn. كما تحتوي على أنشطة وموارد إضافية لكل فصل.

نظرة عامة على الدورة التدريبية

كما يشير عنوان الدورة التدريبية، أن تركيز هذه الدورة التدريبية هو استكشاف مجال الأمن السيبراني. في هذه الدورة التدريبية، سيتم تنفيذ ما يلي:

التعرف على أساسيات الأمان عبر الإنترنت.

التعرف على أنواع مختلفة من البرامج الضارة والهجمات وكيف تحمي المؤسسات نفسها ضد هذه الهجمات.

استكشاف الخيارات المهنية في مجال الأمن السيبراني.

في نهاية هذه الدورة التدريبية، ستكون على دراية أكبر بأهمية أن تكون آمنًا عبر الإنترنت، والعواقب المحتملة للهجمات الإلكترونية، والخيارات المهنية الممكنة في مجال الأمن السيبراني.

الفصل الأول: الحاجة إلى الأمن السيبراني

يوضح هذا الفصل ماهية الأمن السيبراني لماذا يزداد الطلب على متخصصين في الأمن السيبراني؟ ويوضح ما هويتك وبياناتك على الإنترنت، ومكان وجودها، ولماذا تهم مجرمي الإنترنت.

يتناول هذا الفصل أيضا المعلومات، ولماذا يجب حمايتها. يناقش من هم المهاجمون السيبرانيون وماذا يريدون. يجب أن يتمتع المتخصصون في الأمن السيبراني بالمهارات نفسها التي يتمتع بها المهاجمون السيبرانيون، لكن يجب على العاملين في مجال الأمن السيبراني العمل ضمن حدود القانون المحلي والوطني والدولي. كما يجب على المتخصصين في الأمن السيبراني أيضا استخدام مهاراتهم بشكل أخلاقي.

كما يتضمن هذا الفصل محتوى يشرح باختصار ما هي الحرب السيبرانية ولماذا تحتاج الدول والحكومات إلى متخصصين في مجال الأمن السيبراني للمساعدة في حماية مواطنيهم وبنيتهم الأساسية.

ما هو الأمن السيبراني؟

أصبحت شبكة المعلومات الإلكترونية المتصلة جزءًا لا يتجزأ من حياتنا اليومية. حيث تستخدم جميع أنواع المؤسسات، مثل المؤسسات الطبية والمالية والتعليمية، هذه الشبكة للعمل بفعالية. وتستخدم الشبكة عن طريق جمع كميات كبيرة من المعلومات الرقمية ومعالجتها وتخزينها ومشاركتها. ومثلما هو الحال جمع المزيد من المعلومات الرقمية وتقاسمها، لذلك أصبحت حماية هذه المعلومات أكثر حيوية لأمننا القومي واستقرارنا الاقتصادي.

إن الأمن السيبراني هو الجهد المستمر لحماية هذه الشبكات المتصلة معًا وكافة البيانات من الاستخدام غير المصرح به أو الذي يسبب الضرر. على المستوى الشخصي، تحتاج إلى حماية هويتك وبياناتك وأجهزتك الحاسوبية. على مستوى الشركة، يتحمل الجميع مسؤولية حماية سمعة المؤسسة وبياناتها وعملائها. على مستوى الدولة، فإن الأمن القومي وسلامة المواطنين ورفاهيتهم على المحك.

هويتك في وضع الاتصال ووضع عدم الاتصال بشبكة الإنترنت

نظراً لأن المزيد من الوقت يتم إنفاقه على الإنترنت، فإن حالة الاتصال وعدم الاتصال بالإنترنت يمكن ان تؤثر على حياتك. إن هويتك في وضع عدم الاتصال هو الشخص الذي يتفاعل معه أصدقاؤك وعائلتك بشكل يومي في المنزل أو في المدرسة أو في العمل. فهم يعرفون معلوماتك الشخصية، مثل اسمك أو عمرك أو المكان الذي تعيش فيه.

هويتك على الإنترنت هي من أنت في الفضاء السيبراني. هويتك على الإنترنت هي طريقة تقديم نفسك للآخرين عبر الإنترنت. يجب ألا تكشف هذه الهوية عبر الإنترنت سوى كمية محدودة من المعلومات عنك.

يجب توخي الحذر عند اختيار اسم مستخدم أو اسم مستعار لهويتك على الإنترنت. يجب ألا يتضمن اسم المستخدم أي معلومات شخصية. يجب أن يكون شيء مناسب ومحترم. يجب ألا يؤدي اسم المستخدم هذا إلى جعل الغرباء يعتقدون أنك هدف سهل للجرائم الإلكترونية أو اهتمام غير مرغوب فيه.

بياناتك

أي معلومات عنك يمكن اعتبارها بياناتك. يمكن لهذه المعلومات الشخصية أن تعرّفك بشكل فريد كفرد. تتضمن هذه البيانات الصور والرسائل التي تتبادلها مع عائلتك وأصدقائك عبر الإنترنت. ومعلومات أخرى، مثل الاسم ورقم الضمان الاجتماعي وتاريخ ومكان الميلاد أو اسم الأم قبل الزواج، حيث تعتبر معروفة لك وتستخدم للتعرف عليك. يمكن أيضًا استخدام المعلومات مثل المعلومات الطبية والتعليمية والمالية والتوظيفية لتحديد هويتك عبر الإنترنت.

السجلات الطبية

في كل مرة تذهب إلى مكتب الطبيب، يتم إضافة المزيد من المعلومات إلى السجلات الصحية الإلكترونية (EHRs). وتصبح الوصفة الطبية المقدمة من طبيب الأسرة جزءًا من السجلات الصحية الإلكترونية "EHR" الخاصة بك. يتضمن السجل الصحي الإلكتروني "EHR" الخاص بك معلومات عن الصحة البدنية، والصحة العقلية، وغيرها من المعلومات الشخصية التي قد لا تكون ذات صلة بالطب. على سبيل المثال، إذا كانت لديك استشارة أثناء طفولتك عندما حدثت تغييرات كبيرة في الأسرة، فسيكون هذا في مكان ما في سجلاتك الطبية. بالإضافة إلى تاريخك الطبي ومعلوماتك الشخصية، وقد تتضمن السجلات الصحية الإلكترونية "EHR" أيضًا معلومات حول عائلتك.

تستخدم الأجهزة الطبية، مثل برامج اللياقة البدنية، منصة السحابة لتمكين النقل اللاسلكي من تخزين وعرض البيانات السريرية مثل معدلات ضربات القلب وضغط الدم وسكريات الدم. يمكن لهذه الأجهزة توليد كمية هائلة من البيانات السريرية التي يمكن أن تصبح جزءًا من سجلاتك الطبية.

سجلات التعليم

مع تقدمك في التعليم، فإن المعلومات حول الدرجات الخاصة بك ودرجات الاختبار، وحضورك، والدورات التي درستها، وجوائزك، والدرجات التي أخذتها، وأي تقارير تأديبية قد تكون في سجل التعليم الخاص بك. وقد يشمل هذا السجل أيضًا معلومات الاتصال، وسجلات التطعيم والصحة، وسجلات التعليم الخاصة، بما في ذلك برامج التعليم الفردية (IEPs).

السجلات المالية والتوظيف

قد يشتمل سجلك المالي على معلومات حول دخلك ونفقاتك. ويمكن أن تتضمن السجلات الضريبية رواتب الشيكات، وبيانات بطاقات الائتمان، وتقييم الائتمان الخاصة بك وغيرها من المعلومات المصرفية. يمكن أن تتضمن معلومات التوظيف عملك السابق وأدائك.

أين بياناتك؟

كل هذه المعلومات عنك. وهناك قوانين مختلفة تحمي خصوصيتك وبياناتك في بلدك. ولكن هل تعرف مكان بياناتك؟

عندما تكون في مكتب الطبيب، يتم تسجيل المحادثة التي أجريتها مع الطبيب في مخططك الطبي. وبالنسبة لأغراض الفواتير، يمكن مشاركة هذه المعلومات مع شركة التأمين لضمان معرفة قيمة الفواتير والجودة المناسبة. الآن، أصبح هناك جزء من السجل الطبي للزيارة أيضًا في شركة التأمين.

قد تكون بطاقات ولاء العملاء للمتجر وسيلة ملائمة لتوفير المال لشراءاتك. ومع ذلك، يقوم المتجر بتجميع ملف تعريفي لمشترياتك واستخدام تلك المعلومات لمصلحته الخاصة. يظهر الملف الشخصي شرائك لمشتريات من ماركة معينة ونكهة معجون الأسنان بانتظام. يستخدم المتجر هذه المعلومات لاستهداف المشتري بعروض خاصة من شريك التسويق. باستخدام بطاقة الولاء، يكون لدى المتجر والشريك التسويقي ملف تعريف لسلوك عميل.

عندما تقوم بمشاركة صورك عبر الإنترنت مع أصدقائك، هل تعرف من لديه نسخة من الصور؟ نسخ الصور موجودة على أجهزتك الخاصة. قد يمتلك أصدقائك نسخًا من هذه الصور التي تم تنزيلها على أجهزتهم. إذا تمت مشاركة الصور بشكل عام، فقد يكون للغرباء نسخ منها أيضًا. يمكنهم تنزيل تلك الصور أو أخذ لقطات من تلك الصور. ونظرًا لأن الصور تم نشرها عبر الإنترنت، فإنها يتم حفظها أيضًا على أجهزة خوادم موجودة في أجزاء مختلفة من العالم. الآن لم تعد الصور موجودة على أجهزة الحاسوب الخاصة بك.

أجهزة الحاسوب الخاصة بك

لا تقوم أجهزة الحاسوب الخاصة بك بتخزين البيانات الخاصة بك فقط. الآن أصبحت هذه الأجهزة البوابة إلى بياناتك وتوليد معلومات عنك.

ما لم تكن قد اخترت تلقي كشوفات ورقية لجميع حساباتك، فإنك تستخدم أجهزة الحاسوب الخاصة بك للوصول إلى البيانات. إذا كنت ترغب في الحصول على نسخة رقمية من آخر كشف لبطاقة الائتمان، فأنت تستخدم أجهزة الحاسوب لديك للوصول إلى موقع ويب لمصدر بطاقة الائتمان. إذا كنت ترغب في دفع فاتورة بطاقة الائتمان الخاصة بك على الإنترنت، فيمكنك الوصول إلى موقع البنك الخاص بك لتحويل الأموال باستخدام أجهزة الحاسوب الخاصة بك. بالإضافة إلى السماح لك بالوصول إلى معلوماتك، يمكن لأجهزة الحاسوب أيضًا إنشاء معلومات عنك.

مع توفر كل هذه المعلومات عنك على شبكة الإنترنت، أصبحت بياناتك الشخصية متاحة للمتسللين.

إنهم يريدون أموالك

إذا كان لديك أي شيء ذي قيمة، فإن المجرمين يريدون ذلك.

بيانات الاعتماد الخاصة بك على الإنترنت تعتبر ذا قيمة. تمنح بيانات الاعتماد هذه اللصوص إمكانية الوصول إلى حساباتك. قد تعتقد أن الأميال المتراكمة من السفر بالطائرة التي لديك ليست ذات قيمة بالنسبة لمجرمي الإنترنت. فكر في مرة أخرى. بعد اختراق حوالي ١٠،٠٠٠ من الخطوط الجوية الأمريكية والحسابات المتحدة، حجز مجرمو الإنترنت رحلات طيران مجانية باستخدام هذه الوثائق المسروقة. على الرغم من أن الأميال المتراكمة من السفر بالطائرة أعيدت إلى العملاء من قبل شركات الطيران، فإن هذا يدل على قيمة أوراق اعتماد تسجيل الدخول. يمكن للمجرم أيضًا الاستفادة من علاقاتك. يمكنهم الوصول إلى حساباتك على الإنترنت وسمعتك حتى يخدعوك فتظن أنك توصل الأموال إلى أصدقائك أو عائلتك. يمكن للمجرم إرسال رسائل تفيد بأن عائلتك أو أصدقاءك يحتاجون إليك ويطلبون منك إرسال الأموال حتى يتمكنوا من العودة إلى الوطن من الخارج بعد فقدان محافظهم.

المجرمين مبدعون للغاية عندما يحاولون أن يخدعوك لمنحهم المال. إنهم لا يسرقون أموالك فقط، يمكنهم أيضًا سرقة هويتك وإفساد حياتك.

يريدون هويتك

بالإضافة إلى سرقة أموالك لتحقيق مكاسب نقدية على المدى القصير، يريد المجرمون أرباحًا طويلة الأمد من خلال سرقة هويتك.

مع ارتفاع التكاليف الطبية، تزداد سرقة الهوية الطبية. يمكن للصوص الهوية سرقة التأمين الطبي الخاص بك واستخدام الفوائد الطبية الخاصة بك لأنفسهم، وهذه الإجراءات الطبية هي الآن في السجلات الطبية الخاصة بك.

قد تختلف إجراءات إيداع الضرائب السنوية من بلد إلى آخر؛ ومع ذلك، يرى المجرمون الإلكترونيون هذا الأمر كفرصة. على سبيل المثال، يحتاج شعب الولايات المتحدة إلى إيداع ضرائبه بحلول ١٥ أبريل من كل عام. لا تتحقق دائرة الإيرادات الداخلية (IRS) من الإقرار الضريبي مقابل المعلومات من صاحب العمل حتى شهر يوليو. يمكن لسارق الهوية تقديم إقرار ضريبي زائف وجمع المبلغ المسترد. سيلاحظ المدونون الشرعيون عندما يتم رفض طلباتهم بواسطة دائرة الإيرادات الداخلية ."IRS" مع الهوية المسروقة، يمكنهم أيضًا فتح حسابات بطاقات الائتمان وتصعيد الديون باسمك. سيؤدي ذلك إلى الإضرار بتصنيفك الائتماني ويجعل من الصعب عليك الحصول على قروض.

يمكن أن تؤدي بيانات الاعتماد الشخصية أيضًا إلى بيانات الشركة والوصول إلى البيانات الحكومية.

أنواع البيانات

البيانات التقليدية

تشمل بيانات الشركة معلومات الموظفين والملكية الفكرية والبيانات المالية. تتضمن معلومات الموظفين بيانات الطلب، وكشوف الرواتب، وخطابات العروض، واتفاقيات الموظفين، وأي معلومات تستخدم في اتخاذ قرارات التوظيف. تتيح الملكية الفكرية، مثل براءات الاختراع والعلامات التجارية وخطط المنتجات الجديدة، للأعمال التجارية اكتساب ميزة اقتصادية على منافسيها. يمكن اعتبار الملكية الفكرية سرًا تجاريًا. فقدان هذه المعلومات قد يكون كارثًا على مستقبل الشركة. البيانات المالية، مثل بيانات الدخل، والميزانيات العمومية، وبيانات التدفق النقدي للشركة تعطي نظرة ثاقبة على صحة الشركة

.

إنترنت الأشياء والبيانات الضخمة

مع ظهور "إنترنت الأشياء(IoT)"، يوجد الكثير من البيانات لإدارة وتأمين. إنترنت الأشياء عبارة عن شبكة كبيرة من الأشياء المادية، مثل المستشعرات والأجهزة التي تمتد إلى ما بعد شبكة الحاسوب التقليدية. كل هذه الاتصالات، بالإضافة إلى حقيقة أننا قمنا بتوسيع سعة التخزين وخدمات التخزين من خلال السحابة والافتراضية، تؤدي إلى نمو هائل للبيانات. لقد خلقت هذه البيانات مجالًا جديدًا للاهتمام بالتكنولوجيا والأعمال يدعى "البيانات الضخمة". ومع سرعة وحجم وتنوع البيانات الناتجة عن إنترنت الأشياء والعمليات اليومية للأعمال، فإن سرية هذه البيانات وسلامتها وتوافرها أمر حيوي لبقاء المنظمة.

السرية والسلامة والتوفر

تعد إرشادات أمن المعلومات للمؤسسة هي السرية والسلامة والتوفر، حيث تعرف باسم الثلاثي CIA.

تضمن السرية خصوصية البيانات من خلال تقييد الوصول عبر تشفير المصادقة.

تؤكد السلامة أن المعلومات دقيقة وجديرة بالثقة.

يضمن التوفر توافر المعلومات للأشخاص المرخص لهم.

السرية

مصطلح آخر للسرية هو الخصوصية. يجب على سياسات الشركة تقييد الوصول إلى المعلومات بالنسبة إلى الموظفين المصرح لهم والتأكد من أن الأفراد المصرح لهم فقط هم من يشاهدون هذه البيانات. قد تتم تجزئة البيانات وفقًا لمستوى الأمان أو مستوى حساسية المعلومات. على سبيل المثال، لا يجب على مطور برامج Java الوصول إلى المعلومات الشخصية لجميع الموظفين. علاوة على ذلك، يجب على الموظفين تلقي التدريب لفهم أفضل الممارسات في حماية المعلومات الحساسة لحماية أنفسهم والشركة من الهجمات. تتضمن طرق ضمان السرية تشفير البيانات، ومعرف اسم المستخدم وكلمة المرور، والمصادقة الثنائية، وتقليل تعرض المعلومات الحساسة للخطر.

السلامة

تعتبر السلامة هي دقة واتساق وموثوقية البيانات خلال دورة حياتها بالكامل. يجب أن تظل البيانات دون تغيير أثناء النقل ولا تتغير بواسطة كيانات غير مصرح بها. يمكن لأذونات الملفات والتحكم في وصول المستخدم منع الوصول غير المصرح به. يمكن استخدام التحكم في الإصدار لمنع التغييرات غير المقصودة بواسطة المستخدمين المصرح لهم. يجب أن تكون النسخ الاحتياطية متوفرة لاستعادة أي بيانات تالفة، ويمكن استخدام تجزئة المجموع الاختباري للتحقق من تكامل البيانات أثناء النقل.

يستخدم المجموع الاختباري للتحقق من تكامل الملفات، أو سلاسل الأحرف، بعد نقلها من جهاز إلى آخر عبر الشبكة المحلية أو الإنترنت. يتم حساب المجموع الاختباري بوظائف التجزئة. بعض المجاميع الاختبارية الشائعة هي MD5 و SHA-1و SHA-256و SHA-512. تستخدم دالة هاش خوارزمية رياضية لتحويل البيانات إلى قيمة ذات طول ثابت تمثل البيانات. حيث تتواجد القيمة المجزأة ببساطة للمقارنة. لا يمكن استرجاع البيانات الأصلية مباشرة، من القيمة المجزأة. على سبيل المثال، إذا نسيت كلمة المرور الخاصة بك، فلا يمكن استرداد كلمة المرور الخاصة بك من القيمة المجزأة. يجب إعادة تعيين كلمة المرور.

بعد تنزيل أحد الملفات، يمكن التحقق من صحتها بالتحقق من قيم التجزئة من المصدر مع الذي تم إنشاؤه باستخدام أي حاسبة تجزئة. وبمقارنة قيم التجزئة، يمكنك التأكد من أن الملف لم يتم التلاعب به أو تلفه أثناء النقل.

التوفر

الحفاظ على المعدات، وإجراء إصلاحات الأجهزة، والحفاظ على تحديث أنظمة التشغيل والبرامج، وإنشاء نسخ احتياطية تضمن توفر الشبكة والبيانات للمستخدمين المعتمدين. يجب أن تكون الخطط جاهزة للتعافي بسرعة من الكوارث الطبيعية أو الكوارث التي من صنع الإنسان. المعدات أو البرامج الأمنية، مثل الجدران النارية، تحميك من التوقف بسبب هجمات مثل حجب الخدمة .(DoS) يحدث حجب الخدمة عندما يحاول أحد المهاجمين إرباك الموارد بحيث لا تتوفر الخدمات للمستخدمين.

عواقب الاختراق الأمني

إن حماية مؤسسة من كل هجوم إلكتروني محتمل يعتبر أمرًا غير ممكن، وذلك لعدة أسباب. يمكن أن تكون الخبرة اللازمة لإعداد وصيانة الشبكة الآمنة مكلفة. سيستمر المهاجمون دائمًا في العثور على طرق جديدة لاستهداف الشبكات. في نهاية المطاف، سينجح هجوم إلكتروني متقدم ومتعمد. ستكون الأولوية حينئذٍ في مدى سرعة استجابة فريق الأمان للهجوم لتقليل فقدان البيانات ووقت التعطل والعائد.

الآن، أنت تعرف أن أي شيء يتم نشره عبر الإنترنت يمكن أن يبقى على الإنترنت إلى الأبد، حتى إذا تمكنت من محو جميع النسخ الموجودة عندك. إذا تم اختراق أجهزة خوادمك، فيمكن نشر معلومات الموظفين السرية. قد يقوم المخترق (أو مجموعة من المخترقين) بتخريب موقع الشركة الإلكتروني عن طريق نشر معلومات غير صحيحة وإفساد سمعة الشركة التي استغرق بناؤها عدة سنوات. يستطيع المخترقين أيضًا إزالة موقع الويب للشركة مما يؤدي إلى خسارة الشركة للعائد. إذا كان موقع الويب معطلاً لفترات زمنية طويلة، فقد تبدو الشركة غير موثوقة وربما تفقد مصداقيتها. إذا تم اختراق موقع الويب الخاص بالشركة أو الشبكة، فقد يؤدي ذلك إلى تسريب مستندات سرية وكشف أسرار تجارية وملكية فكرية مسروقة. وقد يؤدي فقدان كل هذه المعلومات إلى إعاقة نمو الشركة وتوسعها.

فالتكلفة النقدية للاختراق أعلى بكثير من مجرد استبدال أي أجهزة مفقودة أو مسروقة، والاستثمار في الأمن الحالي وتعزيز الأمن المادي للمبنى. قد تكون الشركة مسؤولة عن الاتصال بجميع العملاء المتأثرين حول الاختراق وقد يتعين عليهم الاستعداد للتقاضي. مع كل هذا الاضطراب، قد يختار الموظفون مغادرة الشركة. قد تحتاج الشركة إلى التركيز بشكل أقل على النمو والمزيد على إصلاح سمعتها.

المثال الأول للاختراق الأمني

اكتشفت إدارة كلمة المرور عبر الإنترنت، لتطبيق LastPass، نشاطًا غير عادي على شبكته في يوليو ٢٠١٥. اتضح أن المتسللين قد سرقوا عناوين البريد الإلكتروني للمستخدم، وتذكيرات كلمة المرور، وتصحيحات التوثيق. ولحسن حظ المستخدمين، لم يتمكن المتسللون من الحصول على خزائن كلمة المرور المشفرة لأي شخص.

على الرغم من وجود اختراق أمني، يمكن لتطبيق LastPass الحفاظ على معلومات حساب المستخدمين. يتطلب تطبيق LastPass التحقق من البريد الإلكتروني أو المصادقة متعددة العوامل كلما كان هناك تسجيل دخول جديد من جهاز غير معروف أو عنوان .IP سيحتاج المتسللون أيضًا إلى كلمة المرور الرئيسية للوصول إلى الحساب.

يتحمل مستخدمو تطبيق LastPass أيضًا بعض المسؤولية في حماية حساباتهم الخاصة. يجب على المستخدمين دائمًا استخدام كلمات المرور الرئيسية المعقدة وتغيير كلمات المرور الرئيسية بشكل دوري. يجب على المستخدمين دائمًا أن يكونوا حذرين من هجمات التصيد الاحتيالي. مثال على هجوم التصيد الاحتيالي هو أن يرسل المهاجم رسائل بريد إلكتروني مزيفة تدعي أنه من تطبيق .LastPass تطلب رسائل البريد الإلكتروني من المستخدمين النقر فوق رابط مضمن وتغيير كلمة المرور. ينتقل الرابط الموجود في البريد الإلكتروني إلى نسخة احتيالية من موقع الويب المستخدم لسرقة كلمة المرور الرئيسية. يجب ألا ينقر المستخدمون مطلقًا على الروابط المضمّنة في بريد إلكتروني. يجب على المستخدمين أيضًا توخي الحذر من تطبيق التذكير بكلمة المرور الخاصة بهم. يجب ألا يعطي تطبيق التذكير بكلمة المرور كلمات المرور الخاصة بك لأحد. الأهم من ذلك، يجب على المستخدمين تمكين المصادقة متعددة العوامل عند توفرها لأي موقع ويب يقدمها.

إذا كان المستخدمون ومقدمو الخدمات يستخدمون الأدوات والإجراءات المناسبة لحماية معلومات المستخدمين، فلا يزال من الممكن حماية بيانات المستخدمين، حتى في حالة حدوث اختراق أمني.

المثال الثاني للاختراق الأمني

عانت شركة Vtech المصنعة للألعاب عالية التقنية للأطفال، من اختراق أمني لقاعدة بياناتها في نوفمبر ٢٠١٥. قد يؤثر على هذا اختراق الملايين من عملاء حول العالم، بما في ذلك الأطفال. كشف اختراق البيانات عن معلومات حساسة بما في ذلك أسماء العملاء وعناوين البريد الإلكتروني وكلمات المرور والصور وسجلات الدردشة.

أصبحت لعبة اللوح هدفًا جديدًا للمتسللين. كان العملاء قد شاركوا الصور واستخدموا ميزات الدردشة من خلال أقراص اللعب. ولم يتم تأمين المعلومات بشكل صحيح، ولم يكن موقع الشركة يدعم الاتصالات الآمنة .SSL على الرغم من أن الخرق لم يكشف عن أي معلومات عن بطاقات الائتمان وبيانات التعريف الشخصية، فقد تم تعليق الشركة في البورصة لأن المخاوف من الاختراق كانت كبيرة.

لم تقم Vtech بحماية معلومات العملاء بشكل صحيح وتم كشفها أثناء الخرق. على الرغم من أن الشركة أبلغت عملاءها بأن كلمات المرور الخاصة بهم قد تم تجزئتها، إلا أنه كان لا يزال بإمكان المتسللين فك رموزها. تم تشفير كلمات المرور في قاعدة البيانات باستخدام دالة تجزئة MD5، ولكن تم تخزين أسئلة الأمان والإجابات في نص عادي. لسوء الحظ، لدى دالة التجزئة MD5 ثغرات أمنية. يمكن للمتسللين تحديد كلمات المرور الأصلية من خلال مقارنة ملايين قيم التجزئة المحسوبة مسبقًا.

ومع تعرض المعلومات في هذا الموقف إلى اختراق للبيانات، يمكن للمجرمين السيبرانيين استخدامها لإنشاء حسابات بريد إلكتروني، والتقدم بطلب للحصول على بطاقات الائتمان، وارتكاب جرائم قبل أن يكون الأطفال كبارًا بما يكفي للذهاب إلى المدرسة. بالنسبة لأولياء أمور هؤلاء الأطفال، يمكن للمجرمين الإلكترونيين أن يتولوا حسابات عبر الإنترنت لأن العديد من الأشخاص يعيدون استخدام كلمات المرور الخاصة بهم على مواقع ويب وحسابات مختلفة.

لم يؤثر الخرق الأمني على خصوصية العملاء فحسب، بل أفسد سمعة الشركة كما أشارت الشركة عندما تم تعليق وجودها في البورصة.

بالنسبة إلى أولياء الأمور، فهي دعوة للاستيقاظ لتكون أكثر يقظة بشأن خصوصية أطفالهم على الإنترنت وطلب أمان أفضل لمنتجات الأطفال. وبالنسبة لمصنعي المنتجات المتصلة بالشبكة، يجب أن يكونوا أكثر عدوانية في حماية بيانات العملاء والخصوصية الآن وفي المستقبل، مع تطور طبيعة الهجوم الإلكتروني.

المثال الثالث للاختراق الأمني

تعتبر Equifax واحدة من الوكالات التي تقدم تقارير عن الائتمان الاستهلاكي الوطني في الولايات المتحدة. تجمع هذه الشركة معلومات عن ملايين العملاء الأفراد والشركات في جميع أنحاء العالم. بناء على المعلومات التي تم تجميعها، درجات الائتمان وتقارير الائتمان تم إنشاؤها حول العملاء. وقد تؤثر هذه المعلومات على العملاء عندما يتقدمون للحصول على قروض وعندما يبحثون عن عمل.

في سبتمبر ٢٠١٧، أعلنت Equifax عن حدوث خرق للبيانات. استغل المهاجمون ثغرة في برنامج تطبيقات الويب .Apache Struts تعتقد الشركة أنه تم الوصول إلى ملايين البيانات الشخصية الحساسة للمستهلكين الأمريكيين من قِبل مجرمي الإنترنت بين مايو ويوليو من عام ٢٠١٧. تتضمن البيانات الشخصية الأسماء الكاملة للعملاء وأرقام الضمان الاجتماعي وتواريخ الميلاد والعناوين ومعلومات أخرى شخصية. هناك أدلة على أن الاختراق ربما أثر على العملاء في المملكة المتحدة وكندا.

أنشأت Equifax موقعًا مخصصًا على الويب يتيح للمستهلكين تحديد ما إذا كانت معلوماتهم قد تعرضت للاختراق، وللتسجيل للحصول على مراقبة الائتمان وحماية سرقة الهوية. باستخدام اسم نطاق جديد، بدلاً من استخدام نطاق فرعي من equifax.com، سمحت هذه الأطراف الشريرة بإنشاء مواقع ويب غير مصرح بها بأسماء مشابهة. يمكن استخدام مواقع الويب هذه كجزء من نظام التصيد الاحتيالي لخداعك لتقوم بتقديم المعلومات الشخصية. وعلاوة على ذلك، قدم موظف من Equifax رابط ويب غير صحيح في وسائل الإعلام الاجتماعية للعملاء القلقين. لحسن الحظ، تمت إزالة هذا الموقع في غضون ٢٤ ساعة. تم إنشاؤه من قبل شخص يستخدمه كفرصة تعليمية لفضح الثغرات الأمنية الموجودة في صفحة استجابة.Equifax

بصفتك مستهلكًا قلقًا، قد تحتاج إلى التحقق بسرعة مما إذا كانت معلوماتك قد تعرضت للاختراق، وبالتالي يمكنك تقليل التأثير. في وقت الأزمات، قد يتم خداعك لاستخدام مواقع ويب غير مصرح به. يجب أن تكون حذرًا بشأن توفير المعلومات الشخصية حتى لا تصبح ضحية مرة أخرى. علاوة على ذلك، فإن الشركات مسؤولة عن الحفاظ على أمان معلوماتنا من الوصول غير المصرح به. تحتاج الشركات إلى تصحيح برامجها وتحديثها بانتظام للتخفيف من استغلال الثغرات المعروفة. ويجب أن يكون موظفوهم متعلمين ومطلعين على إجراءات حماية المعلومات وما يجب فعله في حالة حدوث اختراق.

للأسف، فإن الضحايا الحقيقيين لهذا الاختراق هم الأفراد الذين قد تكون بياناتهم قد تعرضت للاختراق. في هذه الحالة، تتحمل Equifax عبء حماية بيانات المستهلك المجمعة أثناء إجراء فحوصات الائتمان لأن العملاء لم يختاروا استخدام الخدمات المقدمة من .Equifax على المستهلك أن يثق في الشركة لحماية المعلومات التي تجمعها. علاوة على ذلك، يمكن للمهاجمين استخدام هذه البيانات لتحمل هويتك، ومن الصعب جدًا إثبات غير ذلك لأن كلاً من المهاجم والضحية يعرفان نفس المعلومات. في هذه الحالات، يكون أقصى ما يمكنك فعله هو توخي الحذر عند تقديم معلومات تعريف شخصية عبر الإنترنت. تحقق من تقارير الائتمان الخاصة بك بانتظام (مرة واحدة شهريا أو مرة واحدة في كل ربع سنة). قم بالإبلاغ فورًا عن أي معلومات خاطئة، مثل طلبات الائتمان التي لم تبدأها، أو المشتريات على بطاقات الائتمان الخاصة بك التي لم تقم بها.

أنواع المهاجمين

فالمهاجمون هم أفراد أو مجموعات يحاولون استغلال الضعف لتحقيق مكاسب شخصية أو مالية. ويهتم المهاجمون بكل شيء، بدءًا من بطاقات الائتمان وتصميمات المنتجات وأي شيء ذي قيمة

الهواة -يطلق على هؤلاء الأشخاص أحيانًا اسم" script kiddies أطفال السيكربت". عادة ما تكون لديهم مهارات قليلة أو معدومة، وغالبًا ما يستخدمون الأدوات الموجودة أو التعليمات الموجودة على الإنترنت لشن الهجمات. البعض منهم يقوم بذلك لأنه يشعر بالفضول، بينما يحاول آخرون إظهار مهاراتهم وإحداث الضرر. قد يستخدمون الأدوات الأساسية، ولكن النتائج لا تزال مدمرة.

القراصنة -هم مجموعة من المهاجمين الذين يقتحمون أجهزة الحاسوب أو الشبكات للوصول لغايتهم. واعتمادًا على الهدف من عملية الاقتحام، يتم تصنيف هؤلاء المهاجمين على أنها قبعات بيضاء أو رمادية أو سوداء. يقتحم المهاجمون ذوو القبعات البيضاء الشبكات أو أنظمة الحاسوب لاكتشاف نقاط الضعف بحيث يمكن تحسين أمن هذه الأنظمة. يتم هذا الإجراء بإذن مسبق ويتم إبلاغ أي نتائج إلى المالك. ومن ناحية أخرى، يستغل المهاجمون ذوو القبعات السوداء أي ضعف لتحقيق مكاسب شخصية أو مالية أو سياسية غير مشروعة. بينما المهاجمون ذوو القبعات الرمادية في مكان ما بين المهاجمين أصحاب القبعة البيضاء والسوداء. قد يجد المهاجمون ذوو القبعات الرمادية ثغرة في النظام. قد يخبئ قراصنة القبعات الرمادية الضعف أمام مالكي النظام إذا تزامن هذا الإجراء مع أجندتهم. وينشر بعض قراصنة القبعات الرمادية الحقائق حول الثغرة الأمنية على الإنترنت حتى يتمكن المهاجمون الآخرون من استغلالها.

القراصنة المنظمون -هؤلاء القراصنة يكونون من منظمات مجرمي الإنترنت، والمخترقين، والإرهابيين، والقراصنة المدعومين من الدولة. عادة ما يكون مجرمو الإنترنت مجموعة من المجرمين المحترفين يركزون على السيطرة والقوة والثروة. إن المجرمين متطورون ومنظمون للغاية، وقد يقدمون حتى الجرائم الإلكترونية كخدمة للمجرمين الآخرين. يدلي المخترقون النشطاء ببيانات سياسية لخلق الوعي بالقضايا التي تهمهم. يقوم المهاجمون الذين ترعاهم الدولة بجمع المعلومات الاستخبارية أو يقومون بأعمال تخريب نيابة عن حكومتهم. وعادة ما يكون هؤلاء المهاجمون مدربين تدريباً عالياً وممولين بشكل جيد، وتركز هجماتهم على أهداف محددة تعود بالنفع على حكومتهم.

التهديدات الداخلية والخارجية

تهديدات الأمن الداخلي

يمكن أن تنشأ الهجمات من داخل المنظمة أو من خارج المنظمة. يمكن لمستخدم داخلي، مثل الموظف أو شريك في العقد، القيام بهجوم ويمكن أن يكون عن غير قصد أو عن قصد:

- سوء التعامل مع البيانات السرية
- تهديد عمليات الأجهزة خوادم الداخلية أو أجهزة البنية الأساسية للشبكة
- تسهيل الهجمات الخارجية عن طريق توصيل وسائط USB المصابة بنظام الحاسوب الخاص بالشركة
- دعوة غير مقصودة للبرامج الضارة على الشبكة من خلال البريد الإلكتروني أو المواقع الضارة

كما يمكن أن تتسبب التهديدات الداخلية في إحداث ضرر أكبر من التهديدات الخارجية، لأن المستخدمين الداخليين لديهم إمكانية الوصول المباشر إلى المبنى وأجهزته الأساسية. يمتلك الموظفون أيضًا معرفة بشبكة الشركة ومواردها وبياناتها السرية، بالإضافة إلى مستويات مختلفة من امتيازات المستخدم أو الإدارة.

تهديدات الأمن الخارجي

يمكن أن تقوم التهديدات الخارجية من الهواة أو المهاجمين المهرة باستغلال الثغرات الأمنية في الشبكة أو أجهزة الحاسوب، أو استخدام الهندسة الاجتماعية للوصول إلى ما يريده.

ما هي حرب الأنترنت؟

أصبح الفضاء السيبراني بعدًا هامًا آخر للحرب، حيث يمكن للدول أن تنفّذ صراعات دون مواجهات القوات والآلات التقليدية. وهذا يسمح للبلدان ذات الوجود العسكري الأدنى أن يصبح قويًا مثل الدول الأخرى في الفضاء السيبراني. تعتبر حرب الإنترنت صراعًا قائمًا على الإنترنت ينطوي على اختراق أنظمة الحاسوب وشبكات الدول الأخرى. يمتلك هؤلاء المهاجمون الموارد والخبرات اللازمة لشن هجمات ضخمة على الإنترنت ضد دول أخرى لإحداث ضرر أو تعطيل الخدمات، مثل إغلاق شبكة الطاقة الكهربائية.

ومن الأمثلة على المهاجمين الذين ترعاهم الدولة برنامج "Stuxnet" الخبيث المصمم لإتلاف مصنع التخصيب النووي الإيراني. لم تخترق البرامج الخبيثة Stuxnet أجهزة الحاسوب المستهدفة لسرقة المعلومات. بل تم تصميمها لإتلاف المعدات المادية التي كانت تسيطر عليها أجهزة الحاسوب. واستخدم الترميز المعياري المبرمج لأداء مهمة محددة داخل البرامج الخبيثة. واستخدمت شهادات رقمية مسروقة لذلك بدا الهجوم مشروعًا للنظام.

الغرض من حرب الإنترنت

يعد الغرض الأساسي من حرب الإنترنت هو التفوق على الخصوم، سواء كانوا من الدول أو المنافسين.

يمكن لإحدى الدول أن تغزو البنية الأساسية لدولة الأخرى باستمرار، وتسرق أسرار الدفاع، وتجمع المعلومات حول التكنولوجيا لتضييق الفجوات في صناعاتها وقواتها العسكرية. إلى جانب التجسس الصناعي والعسكري، يمكن للحرب السيبرانية أن تخرب البنية التحتية للدول الأخرى وتكلف الأرواح في الدول المستهدفة. على سبيل المثال، يمكن أن يؤدي الهجوم إلى تعطيل شبكة الطاقة في إحدى المدن الرئيسية. وتعطيل حركة المرور. وبذلك سيتوقف تبادل السلع والخدمات. ولا يمكن للمرضى الحصول على الرعاية اللازمة في حالات الطوارئ. قد يتم أيضًا تعطيل الوصول إلى الإنترنت. من خلال التأثير على شبكة الطاقة، يمكن أن يؤثر الهجوم على الحياة اليومية للمواطنين العاديين.

علاوة على ذلك، يمكن للبيانات الحساسة المخترقة أن تعطي المهاجمين القدرة على ابتزاز أفراد داخل الحكومة. قد تسمح المعلومات للمهاجم بالتظاهر بأنه مستخدم مصرح له بالوصول إلى معلومات أو معدات حساسة.

إذا لم تتمكن الحكومة من الدفاع ضد الهجمات الإلكترونية، فقد يفقد المواطنون الثقة في قدرة الحكومة على حمايتهم. يمكن أن تؤدي الحرب السيبرانية إلى زعزعة استقرار الدولة وتعطيل التجارة والتأثير على ثقة المواطنين في حكومتهم دون أن تغزو الدولة المستهدفة فعلياً.

الفصل الأول: الحاجة إلى الأمن السيبراني

شرح هذا الفصل ميزات وخصائص الأمن السيبراني. وأوضح السبب في أن الطلب على المتخصصين في الأمن السيبراني سوف يستمر في الزيادة. يشرح المحتوى سبب كون هويتك وبياناتك الشخصية عبر الإنترنت عرضة للمجرمين السيبرانيين. يقدم لك بعض النصائح حول كيفية حماية هويتك الشخصية عبر الإنترنت وبياناتك.

ويناقش هذا الفصل أيضًا البيانات المؤسسية: ما هي، وأين هي، ولماذا يجب حمايتها. وأوضح من هم المهاجمون السيبرانيون وماذا يريدون. يجب أن يتمتع محترفو الأمن السيبراني بالمهارات نفسها التي يتمتع بها المهاجمون السيبرانيون. يجب على محترفي الأمن السيبراني العمل ضمن حدود القانون المحلي والوطني والدولي. يجب على المتخصصين في الأمن السيبراني أيضا استخدام مهاراتهم بشكل أخلاقي.

وأخيراً، أوضح هذا الفصل باختصار الحرب السيبرانية ولماذا تحتاج الدول والحكومات إلى متخصصين في الأمن السيبراني للمساعدة في حماية مواطنيهم وبنيتهمالأساسية.

الفصل الثاني: الهجمات والمفاهيم والتقنيات

يغطي هذا الفصل الطرق التي يقوم بها المتخصصون في الأمن السيبراني بتحليل ما حدث بعد هجوم إلكتروني. فهو يشرح الثغرات الأمنية في البرامج الأمنية والأجهزة وفئات الثغرات الأمنية المختلفة.

ويناقش الأنواع المختلفة من البرامج الضارة (المعروفة باسم "malware" البرامج الضارة) وأعراض البرامج الضارة. ويتم تغطية الطرق المختلفة التي يمكن أن يتسلل بها المهاجمون إلى النظام، بالإضافة إلى هجمات حجب الخدمة.

معظم الهجمات الإلكترونية الحديثة تعتبر هجمات ممزوجة. تستخدم الهجمات الممزوجة تقنيات متعددة للتسلل إلى النظام ومهاجمته. عندما لا يمكن منع وقوع هجوم، فإن مهمة الأمن السيبراني هي الحد من تأثير ذلك الهجوم.

العثور على الثغرات الأمنية

تمثل الثغرات الأمنية في أي نوع من البرامج أو عيوب الأجهزة. بعد اكتساب معرفة بالثغرة الأمنية، يحاول المتسللين استغلالها. يعتبر **الاستغلال** مصطلح يستخدم لوصف برنامج مكتوب للاستفادة من ثغرة معروفة. ويشار فعل استغلال ثغرة أمنية إلى أنه هجوم. هدف الهجوم هو الحصول على إمكانية الوصول إلى النظام، أو البيانات التي يستضيفها أو الوصول إلى مورد معين.

الثغرات الأمنية في البرامج

وعادة ما يتم تقديم الثغرات الأمنية بالبرامج بسبب أخطاء في نظام التشغيل أو كود التطبيق، وعلى الرغم من كل الجهود التي تبذلها الشركات في البحث عن وتصحيح الثغرات الأمنية بالبرامج، فمن الشائع ظهور ثغرات أمنية جديدة إلى العلن. تصدر Microsoft و Apple وغيرهم من منتجي أنظمة التشغيل تصحيحات وتحديثات كل يوم تقريبًا. تحديثات التطبيق شائعة أيضًا. وغالباً ما تقوم الشركات أو المؤسسات المسؤولة عن تطبيقات مثل مستعرضات الويب وتطبيقات للأجهزة المحمولة وأجهزة خوادم الويب بتحديثها.

في عام ٢٠١٥، تم اكتشاف ثغرة أمنية رئيسية، تسمى SYNful Knock، في Cisco IOS. سمحت هذه الثغرة الأمنية للمهاجمين بالتحكم في أجهزة التوجيه على مستوى المؤسسات، مثل أجهزة توجيه Cisco 1841و٢٨١١ و٣٨٢٥ القديمة. يمكن للمهاجمين بعد ذلك مراقبة جميع اتصالات الشبكة ولديهم القدرة على إصابة أجهزة الشبكة الأخرى. تم إدخال ثغرة أمنية في النظام عند تثبيت إصدار IOSالذي تم تعديله في أجهزة التوجيه. لتجنب ذلك، تحقق دائمًا من سلامة نسخة IOS التي تم تنزيلها وحد من الوصول الفعلي للأجهزة إلى الأفراد المصرح لهم فقط.

الهدف من تحديثات البرامج هو الحفاظ على الوضع الحالي وتجنب استغلال الثغرات الأمنية. في حين أن بعض الشركات لديها فرق اختبار الاختراق مكرسة للبحث، والعثور على الثغرات الأمنية للبرامج والتشخيص قبل أن يتمكن أحد من استغلالها، والباحثين عن الأمن هم طرف ثالث يتخصص أيضا في العثور على الثغرات الأمنية في البرمجيات.

يعتبر Google Project Zero مثالًا رائعًا على هذه الممارسة. بعد اكتشاف عدد من الثغرات الأمنية في مختلف البرامج المستخدمة من قبل المستخدمين النهائيين، شكلت Google فريقًا دائمًا مخصصًا للعثور على ثغرات البرامج. يمكن العثور على بحث Google للأمان."Google Security Research"

الثغرات الأمنية

غالباً ما يتم تقديم ثغرات الأجهزة عن طريق عيوب تصميم الأجهزة. فمثلاً تُعد ذاكرة الوصول العشوائي RAM في الأساس عددًا من المكثفات المُثبَّتة في أماكن قريبة جدًا من بعضها البعض. تم اكتشاف أنه، نظرًا للتقارب، يمكن أن تؤثر التغييرات المستمرة على واحدة من هذه المكثفات على المكثفات المجاورة لها. استنادا إلى هذا الخلل في التصميم، تم إنشاء استغلال يسمى .Rowhammer من خلال إعادة كتابة الذاكرة في نفس العناوين بشكل متكرر، يتيح استغلال Rowhammer إمكانية استرداد البيانات من خلايا ذاكرة العناوين القريبة، حتى إذا كانت الخلايا محمية.

تتعلق الثغرات الأمنية للأجهزة بطرازها، ولا يمكن استغلالها الاستغلال الأمثل من خلال المحاولات العشوائية على الرغم من أن عمليات استغلال الأجهزة تكون أكثر شيوعًا في الهجمات شديدة الاستهداف، إلا أن الحماية التقليدية من البرامج الضارة والأمان المادي توفر حماية كافية للمستخدم اليومي.

تصنيف الثغرات الأمنية

تقع معظم الثغرات الأمنية في إحدى الفئات التالية:

تجاوز سعة المساحة التخزينية المؤقتة – تحدث هذه الثغرة الأمنية عندما تتم كتابة البيانات خارج حدود مساحة التخزين المؤقتة. مساحات التخزين المؤقتة هي مناطق الذاكرة المخصصة لأحد التطبيقات. من خلال تغيير البيانات خارج حدود مساحة التخزين المؤقتة، يصل التطبيق إلى الذاكرة المخصصة لعمليات أخرى. وهذا يؤدي إلى تعطل مفاجئ في النظام، أو اختراق البيانات، أو توفير تصعيد الامتيازات.

عدم التحقق من الإدخال – غالباً ما تعمل البرامج بإدخال بيانات. يمكن أن تحتوي هذه البيانات الواردة في البرنامج على محتوى ضار، مصمم لإجبار البرنامج على التصرف بطريقة غير مقصودة. خذ بعين الاعتبار برنامج يتلقى صورة للمعالج. فيمكن لمستخدم ضار إنشاء ملف صورة له أبعاد صور غير صالحة. ويمكن أن تجبر أبعاد وضعت لتقوم بإجراءات ضارة البرنامج على تخصيص مساحات تخزين بأحجام غير صحيحة وغير متوقعة.

حالات التعارض – هذه الثغرة الأمنية تحدث عندما يعتمد إخراج حدث على مخرجات مرتبة أو محددة زمنياً. تصبح حالة التعارض مصدرًا للضعف عندما لا تحدث الأحداث المطلوبة أو المحددة بتوقيت معين المطلوبة في الترتيب الصحيح أو التوقيت الصحيح.

نقاط الضعف في الممارسات الأمنية – يمكن حماية الأنظمة والبيانات الحساسة من خلال التقنيات مثل المصادقة والترخيص والتشفير. ولا ينبغي للمطورين محاولة إنشاء خوارزميات الأمان الخاصة بهم؛ لأنه من المرجح ستظهر بها ثغرات أمنية. لذا يُنصح بشدة أن يقوم مطورو البرامج باستخدام مكتبات الأمان التي تم إنشاؤها بالفعل واختبارها والتحقق منها.

مشاكل التحكم في الوصول - التحكم في الوصول هو عملية التحكم في تحديد من يقوم بماذا ويمتد من إدارة الوصول الفعلي إلى المعدات لإملاء من له حق الوصول إلى أحد الموارد، مثل الملف، وماذا يمكنهم فعله، مثل القراءة أو التغيير في الملف. يتم إنشاء العديد من الثغرات الأمنية بواسطة الاستخدام غير الصحيح لعناصر التحكم في الوصول.

يمكن التغلب على جميع ضوابط الوصول والممارسات الأمنية تقريبًا إذا تمكن المهاجم من الوصول المادي إلى المعدات المستهدفة. على سبيل المثال، بغض النظر عما قمت بتعيين أذونات الملف إليه، لا يمكن لنظام التشغيل منع أي شخص من تجاوزه وقراءة البيانات مباشرة من القرص. لذا يجب تقييد الوصول المادي ويجب استخدام تقنيات التشفير لحماية البيانات من السرقة أو التلف ولحماية الجهاز والبيانات التي يحتوي عليها.

أنواع البرامج الضارة

اختصار" Malicious Software البرامج الضارة"، هو" malware البرنامج الضار" وهو أي كود يمكن استخدامها لسرقة البيانات أو تجاوز عناصر التحكم في الوصول أو إلحاق الضرر بالنظام أو تعريضه للخطر. فيما يلي بعض الأنواع الشائعة للبرامج الضارة:

برامج التجسس – صممت بهدف التجسس والتتبع وجمع البيانات عن المستخدم. غالبًا ما تتضمن برامج التجسس برامج تعقب النشاطات، وجمع تفاصيل الضغط على لوحة المفاتيح وجمع البيانات. في محاولة للتغلب على الإجراءات الأمنية، تقوم برامج التجسس بتعديل إعدادات الأمان. وغالبًا ما تجمع برامج التجسس نفسها مع البرامج الشرعية أو مع فيروس حصان طروادة."Trojan horse"

برامج الإعلانات المتسللة – هي برامج ضارة صممت بهدف تقديم الإعلانات تلقائياً. وغالباً ما يتم تثبيت برامج الإعلانات المتسللة ببعض إصدارات البرامج. بعض هذه البرامج تكون هدفها الدعاية الاعلانية فقط وبعضها يكون غطاءً مناسباً لبرامج التجسس

" Bot روبوت أو بوت – "تم اشتقاقها من كلمةrobot ، فهي في حقيقة الأمر برامج ضارة صممت لتقوم بتنفيذ إجراء معين بشكل أوتوماتيكي عادة عبر الإنترنت. في حين أن معظم البوتات غير ضارة، إلا أن الاستخدام المتزايد للبوتات الخبيثة يعتبر شبكة الروبوت. تصاب العديد من أجهزة الحاسوب بالبوت التي تتم برمجتها لينتظر بهدوء الأوامر المقدمة من المهاجم.

برامج طلب الفدية – "Ransomware" هي برامج صممت من أجل تعطيل نظام الحاسوب أو البيانات التي تحتوي على ما تملكه حتى يتم إجراء عملية دفع. تعمل تلك البرامج عاده عن طريق تشفير البيانات في جهاز الحاسوب باستخدام مفتاح غير معروف للمستخدم يمكن لبعض الإصدارات الأخرى من برامج طلب الفدية "Ransomware" الاستفادة من الثغرات الأمنية في النظام وإغلاقه. تنتشر برامج طلب الفدية "Ransomware" بواسطة ملف تم تنزيله أو بعض ثغرات البرامج.

برنامج استغلال الخوف – "Scareware" هو نوع من البرامج الضارة المصممة لإقناع المستخدم باتخاذ إجراء محدد بناء على الخوف. يقوم برنامج استغلال الخوف"Scareware" بتكوين إطارات منبثقة تشبه نوافذ حوار نظام التشغيل. تنقل هذه النوافذ رسائل مزورة تفيد بأن النظام في خطر أو يحتاج إلى تنفيذ برنامج معين للعودة إلى التشغيل العادي. في الواقع، لم يتم تقييم أية مشاكل أو اكتشافها، وإذا وافق المستخدم على البرنامج المذكور وتم تنفيذه، فسيتم إصابة نظامه ببرامج ضارة.

برنامج – Rootkit تم تصميم هذا البرنامج الضار لتعديل نظام التشغيل لإنشاء باب خلفي. ثم يستخدم المهاجمون الباب الخلفي للوصول إلى الحاسوب عن بُعد. تستفيد معظم برامج rootkit من الثغرات الأمنية في البرامج لتنفيذ تصعيد الامتيازات وتعديل ملفات النظام. ومن الشائع أيضًا أن تقوم برامج rootkitبتعديل بيانات التحليل الجنائي وأدوات المراقبة، مما يجعل اكتشافها صعباً للغاية. في كثير من الأحيان، يجب أن يتم مسح جهاز حاسوب مصاب بـ rootkit وإعادة تثبيته.

الفيروسات - عبارة عن كود تنفيذي ضار متصل بملفات قابلة للتنفيذ، وغالبًا ما تكون برامج مشروعة. تتطلب معظم الفيروسات تنشيط المستخدم النهائي ويمكن تنشيطها في وقت أو تاريخ محدد. يمكن أن تكون الفيروسات غير ضارة وتعرض صورة ببساطة أو يمكن أن تكون مدمرة، مثل تلك التي تعدل أو تحذف البيانات. يمكن أيضًا أن تكون مبرمجة لتجاوز برامج الحماية والتخفي منها. تنتشر معظم الفيروسات الآن بواسطة محركات أقراص USB أو الأقراص الضوئية أو مشاركات الشبكة أو البريد الإلكتروني.

" **Trojan horse فيروس حصان طروادة** - "هو برنامج خبيث يقوم بعمليات خبيثة تحت ستار العملية المطلوبة. يستغل هذا الكود الخبيث امتيازات المستخدم الذي يشغله. في كثير من الأحيان، يتم العثور على أحصنة طروادة في ملفات الصور والملفات الصوتية أو الألعاب. حصان طروادة يختلف عن الفيروس لأنه يربط نفسه بالملفات غير القابلة للتنفيذ.

الفيروسات المتنقلة – Worms هي شفرة خبيثة تقوم بتكرار نفسها من خلال استغلال الثغرات في الشبكات بشكل مستقل. وعادة ما تؤدي الفيروسات المتنقلة إلى إبطاء الشبكات. وتعمل الفيروسات المتنقلة ذاتيًا، في حين أن الفيروسات لا تعمل إلا من خلال برنامج مُضيف. كما لا تحتاج إلى مشاركة المستخدم إلا في بداية الإصابة. وبعد إصابة المُضيف، يمتلك الفيروس المتنقل القدرة على الانتشار بسرعة كبيرة على الشبكة. تتشارك الفيروسات المتنقلة في تشابه الأنماط. كما أن لديها القدرة على إيجاد الثغرات وهي الطريقة التي تنتشر من خلالها وتتكاثر، وجميعها يحتوي على البيانات الأساسية.

وتعتبر الفيروسات المتنقلة مسؤولة عن بعض الهجمات الأكثر تدميرًا على الإنترنت. في ٢٠٠١ أصاب فيروس Code Red المتنقل ٦٥٨ جهاز خادمًا. وفي غضون ١٩ ساعة، كان الفيروس المتنقل قد أصاب حوالي ٣٠٠٠٠٠ جهاز خادم.

الهجوم الوسيط (MitM) يتيح للمهاجم التحكم في أحد الأجهزة دون معرفة المستخدم. وبهذا المستوى من الوصول، يمكن للمهاجم اعتراض بيانات المستخدم، والتقاطها قبل ترحيلها إلى وجهتها المقصودة. يتم استخدام هجوم MitM على نطاق واسع لسرقة المعلومات المالية. ويوجد العديد من الفيروسات المتنقلة والوسائل المختلفة التي تساعد المهاجم في استخدام إمكانيات.MitM

الهجوم على الأجهزة المحمولة هو نوع من أنواع الهجوم الوسيط، يستغله المستخدم للسيطرة على الأجهزة المحمولة. عند الإصابة، يمكن توجيه معلومات المستخدم الحساسة من الجهاز المحمول وإرسالها إلى المهاجمين. ويعتبرZeuS ، مثالاً على استغلال قدرات MitMo، حيث يقوم المهاجمون في الخفاء بالتقاط رسائل SMS التي تحتوي على التحققات الثنائية المرسلة إلى المستخدمين.

أعراض البرامج الضارة

وفيما يلي أعراض البرامج الضارة الشائعة بغض النظر عن النوع الذي يصيب النظام:

- الزيادة في استخدام المعالج.
- البطء في سرعة الحاسوب.
- توقف الحاسوب أو تعطله في أغلب الأحيان.
- البطء في سرعة تصفح مواقع الإنترنت داخل الشبكة.
- المشاكل الغامضة المتعلقة بالاتصال بالشبكة.
- تعديل الملفات.
- حذف الملفات.
- تواجد الملفات أو البرامج أو الأيقونات على سطح المكتب غير المعروفة.
- هناك تشغيل يحدث لعمليات غير معروفة.
- إيقاف البرامج أو إعادة تشغيل نفسها.
- إرسال رسائل البريد الإلكتروني دون علم المستخدم أو موافقته.

التحايل باستخدام طرق اجتماعية

التحايل بطرق اجتماعية هو عبارة عن هجوم اختراقي يحاول التحكم في الأفراد للقيام بإجراءات معينة أو إفشاء معلومات سرية. وغالباً ما يعتمد هذا التحايل على قابلية الأشخاص للمساعدة ولكنه أيضًا يستغل نقاط ضعفهم. على سبيل المثال، قد يتصل المهاجم بموظف مسؤول بخصوص مشكلة عاجلة تتطلب الوصول الفوري إلى الشبكة. وقد يقنع المهاجم هذا الموظف بأنه عند الرفض سيخفق في مهامه الوظيفية، وقد يقنعه بأنه من طرف شخص ذي رتبة أعلى وظيفيًا، أو قد يستغل طمع الموظف.

فيما يلي بعض من أنواع التحايل باستخدام طرق اجتماعية:

- **التظاهر الخادع** يحدث عندما يتصل المهاجم بأحد الأفراد ثم يستخدم الكذب في محاولة للوصول إلى البيانات المهمة. مثال على ذلك إدعاء المهاجم بأنه يحتاج إلى بيانات شخصية أو مالية من أجل تأكيد هوية المستلم.

- **التتبع** -يحدث ذلك عندما يتبع المهاجم شخصًا مسؤولًا إلى مكان آمن بسرعة.

- **شيء في مقابل شيء** -يحدث عندما يطلب المهاجم معلومات شخصية من مجموعة من الأشخاص مقابل شيء ما، كهدية مجانية.

التلصص على كلمات المرور الخاصة بشبكات Wi-fi

كسر كلمة مرور شبكة Wi-fi هي عملية اكتشاف كلمة المرور المستخدمة لحماية الشبكة اللاسلكية. وفيما يلي بعض التقنيات المستخدمة في اكتشاف كلمة المرور:

التحايل الاجتماعي وهو تحايل المهاجم على الأشخاص الذين يعرفون كلمة السر للحصول عليها.

هجوم القوة الغاشمة وهو محاولة المهاجم استخدام العديد من كلمات المرور المحتملة بغرض تخمين كلمة المرور. على سيبل المثال، إذا كانت كلمة المرور تتكون من ٤ أرقام صحيحة، فسوف يحاول المهاجم جميع التركيبات المحتملة وهي ١٠٠٠٠ تركيبة مختلفة. عادة ما تشمل هجمات القوة الغاشمة ملفًا يحتوي على قائمة بالكلمات. يحتوي هذا الملف النصي على قائمة من الكلمات المقتبسة من قاموس. وبالتالي، يحاول البرنامج استخدام جميع الكلمات والتركيبات الشائعة. ونظراً لاستغراق هجمات القوة الغاشمة الكثير من الوقت، فإن تخمين الكلمات المعقدة يستغرق قدرًا أكبر بكثير من الوقت. من أدوات هجوم القوة الغاشمة التي تتعامل مع كلمات المرور: Ophcrackو L0phtCrackو THCو Hydra و RainbowCrackو.Medusa

مراقبة الشبكة عن طريق ترقب الحزم المرسلة عبر الشبكة والتقاطها، عندها يمكن للمهاجم اكتشاف كلمة المرور إذا لم تكن مشفرة (أو بمعنى آخر إذا كانت مكتوبة كنص عادي). وإذا كانت كلمة المرور مشفرة، فقد يتمكن المهاجم من إظهارها باستخدام أداة للتلصص على كلمة مرور.

التصيد الاحتيالي

يحدث التصيد الاحتيالي عندما يرسل الطرف الضار بريدًا إلكترونيًا مخادعًا متنكراً على أنه مصدر شرعي وموثوق به. وهدف الرسالة هو خداع المستلم لتثبيت البرامج الضارة على أجهزته أو مشاركة معلومات شخصية أو مالية. من أمثلة التصيد الاحتيالي تزوير رسائل البريد الإلكتروني لتبدو وكأنها مرسلة من متجر بيع بالتجزئة يطلب من المستخدم النقر فوق الرابط والحصول على جائزة. وقد ينتقل الرابط إلى موقع مزيف يطلب المعلومات الشخصية، أو قد يقوم بتثبيت الفيروسات.

التصيد محدد الهدف هو هجمة تصيّد احتيالي هادفة. وبينما يستخدم التصيد الاحتيالي ونظيره محدد الهدف رسائل البريد الإلكتروني للوصول إلى الضحايا، فقد يقتصر استخدام التصيد الاحتيالي محدد الهدف فقط على رسائل البريد الإلكتروني الخاصة بشخص معين. كما يبحث المهاجم في اهتمامات الشخص المستهدف قبل إرسال رسالة البريد الإلكتروني. على سبيل المثال، يعرف المهاجم بأن الشخص المستهدف مهتم بالسيارات، ويسعى لشراء طراز محدد من السيارة. عندها يشترك المهاجم في نفس منتدى المناقشات حول السيارات الذي يكون فيه الشخص المستهدف عضواً، ثم يقوم المهاجم بتزوير عرض تجاري على السيارة وإرساله في رسالة بريد إلكتروني إلى الشخص المستهدف.

تحتوي تلك الرسالة على رابط لصور السيارة. وعندما ينقر الشخص المستهدف على الرابط، يتم تثبيت برامج ضارة على جهاز الحاسوب.

استغلال الثغرات الأمنية

ويعتبر استغلال الثغرات الأمنية طريقة أخرى من طرق الاختراق الشائعة. وسيفحص المهاجمون أجهزة الحاسوب للحصول على معلومات حولها. وفيما يلي طريقة شائعة لاستغلال الثغرات الأمنية:

الخطوة الأولى .تجميع المعلومات حول النظام المستهدف. يمكن إجراء ذلك من خلال العديد من الطرق المختلفة مثل فحص المنفذ أو التحايل بطرق اجتماعية. والهدف من ذلك هو الحصول على المعلومات بقدر الإمكان حول الحاسوب المستهدف.

الخطوة الثانية .قد تتضمن تلك المعلومات المناسبة التي تم التعرف عليها في الخطوة الأولى نظام التشغيل وإصداره وقائمة الخدمات القائمة عليه.

الخطوة الثالثة .عند معرفة نظام التشغيل الخاص بالهدف وإصداره، يبحث المهاجم عن أي ثغرات أمنية معروفة متعلقة بهذا الإصدار من نظام التشغيل أو الخدمات الأخرى القائمة عليه.

الخطوة الرابعة .عند اكتشاف الثغرات، يبحث المهاجم عن طرق الاستغلال المكتوبة مسبقاً للاستخدام. وإذا لم توجد طرق استغلال مكتوبة، فعندها يحاول المهاجم كتابة طريقة استغلالية.

المهاجم يستخدم **whois**، وهي عبارة عن قاعدة بيانات عامة على شبكة الإنترنت تحتوي على معلومات حول أسماء المجالات ومن يمتلكها. وكذلك يستخدم أداة **nmap** وهي أداة فحص شائعة للمنافذ. وباستخدام أداة فحص المنافذ، يمكن للمهاجم فحص المنافذ لمعرفة المزيد حول جهاز الحاسوب المستهدف والخدمات قيد التشغيل عليه.

التهديدات المتواصلة المتقدمة

التهديدات المتواصلة المتقدمة(APTs) ، هي من ضمن الطرق التي يتم الاختراق من خلالها. وهي تتكون من عملية متعددة الأنماط طويلة الأمد سرية ومتقدمة على هدف محدد. ونظراً لدرجة تعقيدها ومستوى المهارات المطلوبة، فعادة ما يتم التمويل الجيد لمثل تلك العمليات. وتستهدف APT المؤسسات أو الدول لأسباب تجارية أو سياسية.

ويعتبر الغرض من APT هو نشر البرامج الضارة المخصصة على نظام واحد أو العديد من أنظمة الهدف والتزام التخفي، فهي غالبًا متعلقة بالتجسس من خلال الشبكة. وغالبًا ما يفتقر المهاجم الفردي على مجموعة المهارات أو المصادر أو الصمود لبدء هجماتAPT ، فهي تتكون من عملية متعددة الأنماط بالإضافة إلى العديد من أنواع البرامج الضارة المخصصة التي تصيب الأجهزة المختلفة وتؤدي الوظائف المحددة.

DoS

هجمات رفض الخدمة (DoS) هي نوع من الهجمات التي تتعرض لها الشبكة. وينتج عن هجوم DoS نوعًا من قطع خدمة الشبكة على المستخدمين أو الأجهزة أو التطبيقات. هناك نوعان رئيسيان من هجمات DoS:

إرسال كمية هائلة من البيانات ويحدث ذلك عند استقبال الشبكة أو جهاز المستضيف أو التطبيق لكمية هائلة من البيانات بسرعة لا يمكن التعامل معها. وهذا يتسبب في وجود بطء في الإرسال أو الاستجابة أو تعطل الجهاز أو الخدمة.

الحزم المنسقة بشكل ضار يحدث هذا عندما يتم إرسال حزمة منسقة بشكل ضار إلى جهاز مستضيف أو تطبيق بحيث لا يتمكن المُستقبِل من معالجتها. على سبيل المثال، يمكن للمهاجم إعادة توجيه الحزم التي تحتوي على أخطاء لا يتمكن التطبيق من تحديدها أو يقوم بإعادة توجيه الحزم المنسقة بشكل غير سليم. يؤدي هذا إلى عمل المُستقبِل بشكل بطيء جداً أو إلى تعطيله.

وتشكل هجمات DoS خطراً كبيرًا نظراً لقدرتها على قطع الاتصال بسهولة وعلى إحداث فقد للكثير من الوقت والمال. تكون تلك الهجمات بسيطة نسبياً في إجرائها، حتى من أقل المهاجمين مهارة.

DDoS

هجوم رفض الخدمة الموزع (DDoS) متشابه مع هجوم DoS ولكنه ينشأ من مصادر متعددة منسقة، على سبيل المثال، يمكن متابعة هجوم DDoS كما يلي:

يقوم أحد المهاجمين بإنشاء شبكة مكونة من أجهزة جهاز المضيفات المصابة، تسمى روبوت الشبكة، وتسمى أجهزة جهاز المضيفات المصابة بالأجهزة المُستَغَلة. يتم التحكم في الأجهزة المُستَغَلة من خلال الأنظمة معالجة.

وتفحص أجهزة الحاسوب المُستَغَلة باستمرار المزيد من أجهزة جهاز المضيفات وتنقل لها الإصابة، ومن ثمَّ إنشاء المزيد من الأجهزة المُستَغَلة. ويرشد المهاجم الأنظمة المعالجة لاستغلالها في حمل روبوت الشبكة الموجود في الأجهزة المُستَغَلة لشن هجمة من هجمات DDoS.

تسميم SEO

تعمل محركات البحث مثل Google بتصنيف صفحات الويب وتقديم النتائج ذات الصلة التي تعتمد على استعلامات البحث من المستخدمين. وبناءً على المحتوى ذات الصلة في مواقع الويب، قد تظهر في قائمة نتائج البحث أكثر تقدمًا أو أقل. SEO: هو اختصار لما معناه "تحسين محرك البحث"، وهي عبارة عن مجموعة من التقنيات المستخدمة لتحسين رتبة مواقع الويب عن طريق محرك البحث. وبينما تختص العديد من الشركات مصدر الثقة بتحسين مواقع الويب ووضعها في موضع أفضل، يمكن للمستخدم الضار استخدام SEO لجعل مواقع الويب الضارة تظهر أعلى في نتائج البحث. وتسمى هذه التقنية تسميم SEO.

الهدف الأكثر شيوعاً من تسميم SEO هو زيادة نسبة استخدام المواقع الضارة التي قد تستضيف البرامج الضارة أو تقوم بالتحايل بطرق اجتماعية. ولتعزيز ظهور الموقع أعلى نتائج البحث، يقوم المهاجمون بالاستفادة من مصطلحات البحث الشائعة.

ما هو الهجوم المختلط؟

الهجمات المختلطة هي عبارة عن هجمات تستخدم الأساليب المتعددة لإلحاق الضرر بالأهداف. وباستخدام العديد من أساليب الهجوم المختلفة في نفس الوقت، يحصل المهاجمون على البرامج الضارة التي هي خليط من الفيروسات المتنقلة وفيروسات أحصنة طروادة وبرامج التجسس وبرامج رصد لوحة المفاتيح والرسائل العشوائية وخطط التصيد الاحتيالي. ويكشف هذا الاستخدام المفرط للهجمات المختلطة عن البرامج الضارة الأكثر تعقيداً وبالتالي يعرض بيانات المستخدمين للخطر الجسيم.

يستخدم النوع الأكثر شيوعاً من الهجوم المختلط رسائل البريد الإلكتروني العشوائية أو الرسائل الفورية أو مواقع ويب مصدر ثقة لتوزيع الروابط بحيث يتم تنزيل البرامج الضارة أو برامج التجسس على الحاسوب. ويقوم نوع شائع آخر من الهجمات المختلطة باستخدام DDoS مقترنة بالتصيد الاحتيالي من خلال رسائل البريد الإلكتروني. أولًا يتم استخدام DDoS لتعطيل موقع الويب الخاص ببنك مشهور ثم إرسال رسائل بريد إلكتروني إلى عملاء البنك، للاعتذار عن الإزعاج. ويوجه البريد الإلكتروني المستخدمين إلى موقع طوارئ مزيف حيث يمكن سرقة معلومات تسجيل الدخول الحقيقية الخاصة بهم.

ويمكن وضع معظم الفيروسات المتنقلة الضارة بأجهزة الحاسوب في فئة الهجمات المختلطة التي تشمل Nimbdaو CodeRed و BugBear و Klez و Slammer كما هو موضح بالأسفل:

- وتستخدم بعض الأنواع الأخرى من Nimbda مرفقات البريد الإلكتروني؛ من خلال تنزيل الملفات من جهاز خادم ويب معرض للاختراق؛ وخدمات مشاركة الملفات من (Microsoft على سبيل المثال، مشاركات مجهولة) كطرق للانتشار.
- أما بعض الأنواع الأخرى من Nimbda فلديها القدرة على تعديل حسابات ضيوف النظام لتوفير المهاجم أو التعليمات البرمجية بالامتيازات الإدارية.

وتعتبر الفيروسات المتنقلة Conficker و ZeuS/LICAT من ضمن الهجمات المختلطة. يستخدم Confickerجميع طرق التوزيع التقليدية.

ما هو تخفيف الأثر؟

وبينما تعي معظم الشركات الناجحة حاليًا بالمشاكل الأمنية الشائعة بحيث تبذل جهدًا كبيرًا للتصدي لها، إلا أنه لا توجد ممارسات أمنية بكفاءة ١٠٠%. ويتحتم أيضًا على الشركات والمنظمات الاستعداد لاحتواء الخسائر، لأن الاختراق يحدث عندما تكثر الغنيمة.

من المهم أيضًا فهم أن تأثير الاختراق لا يتعلق فقط بالناحية التقنية مثل سرقة البيانات أو تدمير قواعد البيانات أو تعطيل الحقوق الملكية الفكرية، بل يمتد التلف أيضًا ليشمل سمعة الشركة. والرد على اختراق البيانات هي عملية ديناميكية بشكل كبير.

فيما يلي بعض المقاييس الهامة كما يراها خبراء الأمن، التي يجب أن تتخذها الشركات عند رصد الاختراقات الأمنية:

- الإخطار بالمشكلة. من الناحية الداخلية، يجب إخطار الموظفين بالمشكلة وحثهم على اتخاذ الإجراءات. ومن الناحية الخارجية، يجب إخطار العملاء من خلال التواصل المباشر والتصريحات الرسمية. فالتواصل يخلق جوًا من الشفافية، التي تعتبر أمرًا أساسيًا في هذا النوع من الحالات.
- تحلى بالنزاهة والثقة في حالة تعرض الشركة للخطر.
- الإدلاء بالتفاصيل. شرح أسباب حدوث هذا الموقف وتوضح الأشياء المهددة. من المتوقع أيضًا أن الشركة تهتم بخدمات الحماية من مخاطر سرقة الهوية للعملاء المتأثرين.

- فهم المسببات والعوامل المساعدة في حدوث الاختراق. توظيف خبراء التحليل لبحث التفاصيل والتعرف عليها، إذا اقتضى الأمر.
- تطبيق الدروس المستفادة من التحريات التحليلية لضمان عدم حدوث اختراقات مشابهة في المستقبل.
- التأكد من أن جميع الأنظمة نظيفة ولم يتم تثبيت البرامج التسللية عليها، والتأكد من عدم اختراق أي شيء آخر. سيحاول المهاجمون غالباً ترك البرامج التسللية لتسهيل الاختراقات في المستقبل. تأكد من عدم حدوث ذلك.
- تثقيف الموظفين والشركاء والعملاء بطرق منع الاختراقات المستقبلية.

الفصل الثاني: الهجمات: المفاهيم والتقنيات

تناول هذا الفصل الطرق التي يحلل من خلالها خبراء الأمان السيبراني الأشياء التي حدثت بعد الهجوم. فهو يشرح نقاط الضعف في البرامج الأمنية والأجهزة والفئات المختلفة للثغرات الأمنية.

شرح الأنواع المختلفة للبرامج الضارة وأعراضها. تشمل بعض البرامج الضارة التي تمت مناقشتها الفيروسات والفيروسات المتنقلة وأحصنة طروادة وبرامج التجسس، وبرامج الإعلانات المتسللة وغيرهم.

وتم تناول الطرق المختلفة التي من خلالها يمكن للمهاجمين التسلل إلى الأنظمة، بما في ذلك التحايل بطرق اجتماعية واختراق كلمة مرور شبكة Wi-fi، والتصيد الاحتيالي واستغلال الثغرات الأمنية. كما تم شرح الأنواع المختلفة لهجمات رفض الخدمة أيضا.

تستخدم الهجمات المختلطة تقنيات متعددة للتسلل إلى النظام ومهاجمته. ويمكن اعتبار العديد من الفيروسات المتنقلة الضارة بأنها هجمات مختلطة، وهي تشمل CodeRed و BugBear و Klez و slammer. وفي حالة عدم إمكانية التصدي للهجمات، فإن من مهمة الشخص المحترف في مجال الأمان السيبراني التخفيف من أثر هذا الهجوم.

الفصل الثالث: حماية بياناتك وخصوصيتك

يركز هذا الفصل على الأجهزة الشخصية والبيانات الشخصية. ويتضمن النصائح لحماية الأجهزة وإنشاء كلمات مرور واستخدام الشبكات اللاسلكية بأمان. كما يناقش الحفاظ على البيانات بشكل أمن.

البيانات الشخصية على شبكة الإنترنت بها من المطامع ما يغري المجرمين. يتناول هذا الفصل بإيجاز أساليب المصادقة للمساعدة في الحفاظ على البيانات بشكل أمن. ويتناول أيضا طرق تحسين أمان البيانات عبر الإنترنت والنصائح حول الممارسات المستحبة ومثيلتها التي يجب تجنبها على الإنترنت.

حماية أجهزة الحوسبة

تقوم أجهزة الحوسبة بتخزين البيانات كما تعتبر هي المدخل إلى الحياة الشخصية عبر الإنترنت. فيما يلي قائمة قصيرة لخطوات يمكن اتباعها لحماية أجهزة الحاسوب من الاختراق:

- **ابق جدار الحماية على وضع التشغيل** -سواءً كان برنامج جدار حماية أو جهاز جدار حماية في جهاز التوجيه، يجب تشغيل جدار الحماية وتحديثه لمنع المتخترقين من الوصول إلى بياناتك الشخصية أو بيانات الشركة.
- **استخدم برامج الحماية من الفيروسات وبرامج التجسس** -يتم تثبيت البرامج الضارة، مثل الفيروسات وأحصنة طروادة والفيروسات المتنقلة وبرامج الفدية وبرامج التجسس، على أجهزة الحاسوب دون إذن منك، من أجل الوصول إلى جهاز الحاسوب والبيانات. يمكن للفيروسات أن تتسبب في تدمير البيانات أو إبطاء الحاسوب أو الاستيلاء عليه. ومن خلال السماح لمرسلي البريد العشوائي بنشر رسائل البريد الإلكتروني باستخدام حسابك الشخصي، تسيطر الفيروسات على جهاز الحاسوب، وهي طريقة من ضمن الطرق. ويمكن لبرامج التجسس مراقبة أنشطتك عبر الإنترنت أو جمع معلوماتك الشخصية، أو إظهار العديد من الإعلانات المنبثقة غير المرغوبة في مستعرض الويب إذا كنت متصلاً. وتكمن القاعدة الجيدة في تنزيل البرامج من المواقع الموثوق بها في المقام الأول لتجنب الحصول على برامج التجسس. تم تصميم برامج الحماية من الفيروسات لفحص الحاسوب والبريد الإلكتروني الوارد للبحث عن الفيروسات وحذفها. عادةً ما تشتمل برامج الحماية من الفيروسات على برامج الحماية من التجسس. حافظ على تحديث البرامج لحماية جهاز الحاسوب من أحدث البرامج الضارة.
- **قم بإدارة نظام التشغيل والمتصفح** -يحاول المتسللون دائمًا الاستفادة من نقاط الضعف في أنظمة التشغيل ومتصفحات الويب. لحماية جهاز الحاسوب والبيانات، قم بتعيين إعدادات الأمان على الحاسوب وعلى المستعرض إمَّا أمان متوسط أو أعلى. قم بتحديث نظام تشغيل جهاز

الحاسوب بما في ذلك مستعرضات الويب وقم بتنزيل أحدث تصحيحات البرامج وتحديثات الأمان من البائعين وتثبيتها بشكل منتظم.

- **قم بحماية جميع أجهزتك** -يجب أن تكون أجهزة الحوسبة، سواء كانت أجهزة سطح مكتب أو أجهزة حاسوب محمولة أو أجهزة لوحية أو هواتف ذكية، محمية بكلمة مرور لمنع الوصول غير المصرح به. ينبغي تشفير المعلومات المخزنة، خاصة المتعلقة بالبيانات السرية أو المهمة. بالنسبة للأجهزة المحمولة، قم فقط بتخزين المعلومات الضرورية في حالة سرقة هذه الأجهزة أو فقدانها عندما تكون بعيدًا عن منزلك. إذا تم اختراق أحد الأجهزة، يمكن للمخترقين الوصول إلى جميع بياناتك من خلال موفر خدمة التخزين عبر السحابة، مثل خدمة iCloud أو Google drive.

تتسبب أجهزة إنترنت الأشياء خطرًا أكبر من أجهزة الحوسبة الأخرى. بينما سطح المكتب والحاسوب المحمول والأنظمة الأساسية المحمولة تستقبل الكثير من التحديثات، لا تزال معظم أجهزة إنترنت الأشياء تحتفظ بالبرامج الثابتة الأصلية. إذا تم العثور على الثغرات الأمنية في البرامج الثابتة، فمن المرجح أن يظل الجهاز بتلك الحالة. وما يزيد الأمر سوءً، هو تصميم أجهزة إنترنت الأشياء غالبًا بغرض الاتصال بالمنزل، ومن ثمَّ تتطلب الوصول إلى الإنترنت. للوصول إلى الإنترنت، تعتمد معظم الشركات المصنعة لأجهزة إنترنت الأشياء على الشبكة المحلية الخاصة بالعميل. النتيجة هي أن أجهزة إنترنت الأشياء معرضة بشكل كبير للاختراق، وعندما يحدث ذلك، تتيح الوصول إلى شبكة العميل المحلية وبياناته. وأفضل طريقة للحماية من هذا السيناريو هو التعامل مع أجهزة إنترنت الأشياء باستخدام شبكة معزولة، ومشاركتها فقط مع أجهزة إنترنت الأشياء الأخرى.

استخدم الشبكات اللاسلكية بأمان

تسمح الشبكات اللاسلكية للأجهزة التي تمتلك خاصية Wi-fi، مثل أجهزة الحاسوب المحمولة وأجهزة الحاسوب المكتبية، بالاتصال بالشبكة عن طريق معرف الشبكة، المعروف باسم معرف مجموعة الخدمات .(SSID) ولمنع المتسللين من الدخول على الشبكة اللاسلكية المنزلية، يجب تغيير معرف SSIDالمعين مسبقاً وكلمة المرور الافتراضية للواجهة الإدارية المستندة إلى المتصفح. سيكون المهاجمون على دراية بهذا النوع من معلومات الوصول الافتراضية. وبشكل اختياري، يمكن أيضا تكوين الموجه اللاسلكي على عدم بثSSID ، وبذلك يقوم بإضافة حاجز إضافي أمام اكتشاف الشبكة. ومع ذلك، لا يمكن اعتبار ذلك بالأمان الكافي للشبكات اللاسلكية. علاوة على ذلك، يجب تشفير الاتصال اللاسلكي من خلال تمكين الأمان اللاسلكي وميزة تشفير WPA2 على الموجه اللاسلكي. حتى مع تمكين تشفير WPA2، لا تزال الشبكة اللاسلكية معرضة للاختراق.

في أكتوبر عام ٢٠١٧، تم اكتشاف وجود خطأ أمني في بروتوكول WPA2 يتيح هذا الخطأ للمتسلل فك التشفير بين الموجه اللاسلكي وبين العميل الذي يستخدمه، والسماح له بالوصول إلى عملية نقل البيانات والتحكم فيها. يمكن استغلال تلك الثغرة الأمنية باستخدام **هجمات إعادة تثبيت المفتاح** .(KRACK) فهي تؤثر على جميع شبكات Wi-fi الحديثة المحمية. للحد من خطورة المهاجم، يتحتم على المستخدم تحديث كافة المنتجات المتأثرة: أجهزة التوجيه اللاسلكية وأي أجهزة لا سلكية، مثل أجهزة الحاسوب المحمول والأجهزة المتنقلة، بمجرد توفر تحديثات الأمان. وقد يقوم الاتصال السلكي بالحد من هذه الثغرة الأمنية، بالنسبة لأجهزة الحاسوب المحمولة أو الأجهزة أخرى المجهزة ببطاقة NIC السلكية. علاوة على ذلك، يمكن أيضا استخدام خدمة VPN الموثوق بها لمنع الوصول غير المرخص به للبيانات أثناء استخدام الشبكة اللاسلكية.

تسمح لك نقطة الاتصال العامة لاتصال Wi-fi بالوصول إلى معلوماتك عبر الإنترنت وتصفح الشبكة، عندما تكون خارج المنزل. ومع ذلك، فمن الأفضل عدم الوصول إلى الشبكات اللاسلكية العامة أو إرسال أي معلومات شخصية حساسة عليها. تحقق من تكوين جهاز الحاسوب بمشاركة الملفات والوسائط وأنه يتطلب مصادقة المستخدم من خلال التشفير. لمنع أي شخص من اعتراض المعلومات الخاصة بك (تعرف باسم "التنصت") أثناء استخدام الشبكات اللاسلكية العامة، استخدم أنفاق VPNالمشفرة وخدماتها. توفر لك خدمة VPN وصولاً آمناً إلى الإنترنت، من خلال الاتصال المشفر بين الحاسوب وبين جهاز خادم (VPN) من الجهة موفرة الخدمة. وباستخدام أنفاق (VPN) المشفرة، لا يمكن فك شفرتها، حتى في حالة اعتراض نقل البيانات.

تأتي العديد من الأجهزة المتنقلة مثل الهواتف الذكية وأجهزة الحاسوب اللوحية مزودة ببروتوكول Bluetooth اللاسلكي. تسمح هذه الإمكانية للأجهزة المزودة بتقنية Bluetooth بالاتصال ببعضها بعضًا ومشاركة المعلومات. ولسوء الحظ، يمكن أن يستغل المتسللون تقنية Bluetooth للتجسس على بعض الأجهزة، وإنشاء عناصر التحكم في الوصول عن بُعد، وتوزيع البرامج الضارة واستنزاف البطاريات. لتجنب مثل هذه المشكلات، قم بإيقاف تشغيل تقنية Bluetooth في حالة عدم استخدامه.

استخدم كلمات مرور مميزة لكل حساب عبر الإنترنت

قد تمتلك لأكثر من حساب على الإنترنت، ولذلك يجب أن يكون لكل حساب كلمة مرور غير مكررة. قد تكون أي من تلك الكلمات صعبة التذكر. ولكن العواقب المترتبة على عدم استخدام كلمات مرور قوية وغير مكررة يجعلك أنت وبياناتك عرضة للمهاجمين عبر الإنترنت. استخدام كلمة المرور ذاتها لجميع الحسابات عبر الإنترنت يشبه استخدام نفس المفتاح لجميع الأبواب المغلقة، إذا تمكن أحد المهاجمين من الحصول على المفتاح، فسوف يتمكن من الوصول إلى كل شيء تملكه. إذا تمكنت العناصر الإجرامية من الحصول على كلمة المرور الخاصة بك من خلال التصيد الاحتيالي على سبيل المثال، فسوف يحاولون الوصول إلى حساباتك الأخرى عبر الإنترنت. إذا كنت تستخدم كلمة مرور واحدة فقط لجميع الحسابات، فسيمكنهم الوصول إلى جميع حساباتك، وسرقة جميع البيانات ومسحها أو قد ينتحلون شخصيتك.

نحن نستخدم العديد من الحسابات عبر الإنترنت التي تحتاج إلى كلمات المرور والتي يصبح من الصعب تذكرها. حل واحد لتجنب إعادة استخدام كلمات المرور أو استخدام كلمات مرور ضعيفة هو استخدام برنامج لإدارة كلمات المرور. فهذا البرنامج يقوم بتشفير جميع كلمات المرور المختلفة والمعقدة. ثم يساعدك على تسجيل الدخول إلى الحسابات تلقائيًا عبر الإنترنت. وما عليك إلا تذكر كلمة المرور الرئيسية للوصول إلى برنامج إدارة كلمات المرور ثم إدارة جميع الحسابات وكلمات المرور.

نصائح لاختيار كلمات المرور الجيدة:

- لا تستخدم كلمات القاموس أو أسماء بأية لغة
- لا تستخدم الأخطاء الإملائية الشائعة لكلمات القاموس
- لا تستخدم أسماء أجهزة الحاسوب أو أسماء الحسابات
- إذا أمكن، استخدم أحرف خاصة، مثل (* & ^ % $ # @ !)
- استخدم كلمة مرور مكونة من عشرة أحرف أو أكثر

استخدم جمل المرور بدلاً من كلمات المرور

لمنع الوصول المادي غير المصرح به إلى أجهزة الحاسوب، استخدم جمل المرور، بدلاً من كلمات المرور. من السهل إنشاء جملة مرور طويلة بدلًا من كلمات مرور، نظراً لأنها على شكل جمل وليست كلمات. وكلما زاد طول الجمل قلّ التعرض لهجمات القوة الغاشمة أو تلك المستخدمة لقوائم الكلمات. علاوة على ذلك، قد تكون جمل المرور أسهل من ناحية التذكر، خاصةً إذا كنت مطالبًا بتغيير كلمات المرور باستمرار. فيما يلي بعض النصائح حول اختيار كلمات مرور أو جمل المرور الجيدة:

نصائح لاختيار جمل المرور الجيدة:

- اختر جملة لها معنى بالنسبة لك
- أضف رموزًا خاصة، مثل ( ) * & ^ % $ # @ !
- كلما كانت أطول كلما كان أفضل
- تجنب الجمل المشهورة أو الشائعة، مثل كلمات الأغاني المعروفة

مؤخرا، قام المعهد الوطني للمعايير والتكنولوجيا (NIST) بالولايات المتحدة بنشر متطلبات كلمات المرور المعدلة. معايير NIST مخصصة للتطبيقات الحكومية ولكنها يمكن أن تكون مقياسًا للتطبيقات الأخرى أيضًا. وتسعي الإرشادات الجديدة لتوفير تجربة أفضل للمستخدم ونقل عبء التحقق من المستخدم إلى مقدمي الخدمات.

ملخص للإرشادات الجديدة:

- 8أحرف كحد أدنى للطول، ولكن لا تزيد عن ٦٤ حرفًا
- لا تستخدم كلمات مرور عامة يسهل تخمينها، مثل كلمة المرور: abc123
- عدم استخدام قواعد التأليف، مثل الحاجة إلى تضمين أحرف وأرقام صغيرة وأخرى كبيرة
- تحسين دقة الكتابة عن طريق السماح للمستخدم برؤية كلمة المرور أثناء الكتابة
- جميع حروف الطباعة والمسافات مسموح بها
- لا تلميحات لكلمات المرور
- عدم انتهاء صلاحية كلمة مرور دوريًا أو عشوائيًا
- عدم استخدام مصادقة تستند إلى المعرفة، مثل المعلومات من الأسئلة السرية المشتركة، أو البيانات التسويقية أو سجل المعاملات

حتى مع الوصول إلى أجهزة الحاسوب وتأمين الأجهزة المتصلة بالشبكة، من المهم أيضا حماية البيانات والمحافظة عليها.

قم بتشفير بياناتك

يجب دائماً تشفير البيانات. قد تظن بأنه لا حاجة للتشفير ما دمت لا تمتلك الأسرار أو الأشياء التي تريد إخفائها. وقد تظن أنه لا أحد يهتم بالحصول على بياناتك. على الأرجح، من المحتمل أن هذا ليس صحيحًا.

هل أنت مستعد لعرض جميع الصور والمستندات على الأشخاص الغرباء؟ هل أنت مستعد لمشاركة المعلومات المالية المخزنة على الحاسوب مع أصدقائك؟ هل تريد الإفصاح عن كلمات مرور الحسابات ورسائل البريد الإلكتروني للعامة؟

قد يصبح الأمر أكثر إشكالية إذا أصابت التطبيقات الضارة جهاز الحاسوب أو الهاتف المحمول وسرقت المعلومات الهامة، مثل أرقام الحسابات وكلمات المرور والمستندات الرسمية الأخرى. ويمكن أن يؤدي هذا النوع من المعلومات إلى سرقة الهوية أو الاحتيال أو طلب الفدية. قد تقرر العناصر الإجرامية تشفير البيانات وجعلها غير قابلة للاستخدام حتى تدفع الفدية.

ما المقصود بالتشفير؟ التشفير هو عملية تحويل المعلومات إلى صيغ بحيث يتعذر على الأطراف غير المصرح لهم قراءتها. ويمتلك الأشخاص الموثوق بهم فقط (الذين يمتلكون المفاتيح السرية أو كلمات المرور) القدرة على تشفير البيانات والوصول إليها في صيغتها الأصلية والتشفير في حد ذاته لا يمنع أي شخص من توقع البيانات. بل يمكنه فقط منع الأشخاص غير المرخص لهم من عرض المحتوى أو الوصول إليه.

وتستخدم البرامج لتشفير الملفات والمجلدات وحتى محركات الأقراص بالكامل.

ويعد نظام تشفير الملفات (EFS) ميزة من ميزات نظام التشغيل Windows التي يمكنها تشفير البيانات. ويرتبط نظام EFS مباشرة بحساب مستخدم معين. والمستخدم الذي قام بتشفير البيانات هو وحده الذي يمكنه الوصول إليها بعد تشفيرها باستخدام نظام .EFS لتشفير البيانات باستخدام نظام EFSفي جميع إصدارات نظام التشغيلWindows ، اتبع هذه الخطوات:

الخطوة الأولى .حدد ملفًا أو مجلدًا واحدًا أو أكثر.

الخطوة الثانية .انقر بزر الفأرة الأيمن على **خصائص** البيانات المحددة.

الخطوة الثالثة .انقر فوق **خيارات متقدمة...**

الخطوة الرابعة .حدد خانة الاختيار **تشفير المحتويات لتأمين البيانات.**

الخطوة الخامسة .يتم عرض الملفات والمجلدات التي تم تشفيرها باستخدام نظام EFS باللون الأخضر.

انسخ بياناتك احتياطياً

قد تحدث مشكلة في محرك الأقراص الثابتة مما يؤدي إلى عدم الوصول للبيانات. أو قد تفقد الحاسوب المحمول. أو يتم سرقة الهاتف الذكي. وقد تمسح النسخة الأصلية من المستندات الهامة. وجود نسخة احتياطية يمنع فقد البيانات التي يصعب تعويضها، مثل الصور الفوتوغرافية العائلية. لإجراء النسخ الاحتياطي للبيانات بشكل صحيح، أنت بحاجة إلى موقع تخزين إضافي للبيانات ويجب نسخ البيانات إلى هذا الموقع بشكل منتظم وتلقائي.

قد يكون الموقع الإضافي للملفات الاحتياطية على الشبكة المنزلية أو موقع ثان، أو على السحابة. من خلال تخزين النسخ الاحتياطي للبيانات محلياً، يمكنك التحكم في البيانات بشكل تام. يمكنك الاختيار بين نسخ البيانات إلى جهاز التخزين المرفق بالشبكة (NAS) أو محرك أقراص ثابتة خارجي، أو ربما تحديد المجلدات الهامة فقط للنسخ الاحتياطي على الأقراص المضغوطة أو أقراص Dvd أو محركات الأقراص المصغرة أو أشرطة التخزين. في تلك الحالة، أنت المالك وأنت المسئول بشكل تام عن تكلفة معدات أجهزة التخزين وصيانتها. وإذا كان يمكنك الاشتراك في خدمة التخزين عبر السحابة، فإن التكلفة تعتمد على مقدار مساحة التخزين المطلوبة. مع خدمة التخزين عبر السحابة مثل خدمات Amazonللويب(AWS) ، يتاح لك الوصول إلى بيانات النسخ الاحتياطي طالما أن لديك حق الوصول إلى حسابك. وعند الاشتراك في خدمات التخزين عبر الإنترنت، فقد تحتاج لتكون أكثر تحديداً حول البيانات الاحتياطية نظراً لتكلفة التخزين وعملية نقل البيانات المستمرة عبر الإنترنت. من فوائد تخزين النسخ الاحتياطية في المواقع البديلة هي الأمان في حالة حدوث حريق أو سرقة أو الكوراث الأخرى بخلاف تعطل جهاز التخزين.

حذف البيانات نهائياً

عند نقل ملف إلى سلة المحذوفات أو سلة المهملات وحذفه بشكل دائم، فهذا الملف لا يمكن الوصول إليه فقط من نظام التشغيل. بل يمكن لأي شخص مجهز بالأدوات التحليلية السليمة استعادة الملف نظرًا لما خلفه من أثر مغناطيسي على محرك الأقراص الصلب.

لمسح البيانات بحيث لا تصبح قابلة للاستعادة، يجب استبدال تلك البيانات بـ ٠، و١ عدة مرات. ولمنع استعادة الملفات المحذوفة، قد تحتاج إلى استخدام أدوات مصممة خصيصا للقيام بذلك. يتميز برنامج SDelete من Microsoft لنظام التشغيل Vista وما أحدث بالقدرة على إزالة الملفات الهامة تمامًا. كما يختص برنامج Shred لنظام التشغيل Linux وميزة إفراغ سلة المهملات لنظام التشغيل Mac OSX ببعض الأدوات المطلوبة لتوفير الخدمات المشابهة.

الطريقة الوحيدة للتأكد من أن البيانات أو الملفات غير قابلة للاستعادة هي تدمير جهاز التخزين أو محرك الأقراص الثابتة. لقد كان المجرمين حمقى في ظنهم بأن ملفاتهم غير قابلة للاختراق أو الاستعادة.

بالإضافة إلى تخزين البيانات على محركات الأقراص الثابتة الخاصة بك، يمكن أيضًا أن يتم تخزين البيانات عبر الإنترنت في السحابة. ستحتاج أيضا إلى حذف تلك النسخ. حاول أن تفكر لمدة دقيقة واحدة، "أين يمكنني حفظ البيانات؟ هل تم نسخها احتياطياً في مكان ما؟ هل تم تشفيرها؟ عندما تحتاج إلى حذف البيانات أو التخلص من محرك الأقراص الثابتة أو الحاسوب، اسأل نفسك، "هل قمت بحماية البيانات لمنع الأشخاص الخطأ من الحصول عليها؟"

المصادقة الثنائية

تستخدم خدمات الإنترنت الشائعة، مثل Google و Facebook و Twitter و LinkedIn و Appleو Microsoft المصادقة الثنائية لتعزيز الأمان الخاص بتسجيل الدخول للحسابات. بالإضافة إلى اسم المستخدم وكلمة المرور، أو رقم التعريف الشخصي (PIN) أو النمط، تتطلب المصادقة الثنائية رمزًا مميزًا آخر مثل:

- **الأشياء المادية** -بطاقة الائتمان أو بطاقة الصراف الآلي أو الهاتف
- **فحص بالقياس الحيوي** -بصمات الأصابع أو بصمات الكف وكذلك تقنيات التعرف على الوجه أو الصوت

حتى مع المصادقة الثنائية، لا يزال المخترقين قادرين على الوصول إلى الحسابات عبر الإنترنت من خلال هجمات مثل هجمات التصيد الاحتيالي والبرامج الضارة والتحايل بطرق اجتماعية.

OAuth 2.0

المصادقة المفتوحة (OAuth) هو بروتوكول قياسي مفتوح يتيح لبيانات المستخدم النهائي اعتماد الوصول إلى تطبيقات الإنترنت دون إظهار كلمة المرور. يعمل OAuth كوسيط لتحديد إمكانية السماح للمستخدمين بالوصول إلى تطبيقات الإنترنت. على سبيل المثال، نفترض أنك تريد الوصول إلى تطبيق الويبXYZ ، ولم يكن لديك حساب مستخدم للوصول إلى هذا التطبيق. لهذا، يحتوي XYZعلى خيار للسماح بتسجيل الدخول باستخدام بيانات الاعتماد من موقع ويب التواصل الاجتماعي .ABC وبالتالي يمكنك الوصول إلى موقع الويب باستخدام بيانات تسجيل الدخول الخاصة بموقع التواصل الاجتماعي.

ولينجح ذلك، تم تسجيل 'ABC' مع تطبيق 'XYZ' وبالتالي أصبح تطبيق معتمد. وعند الوصول إلى XYZ، يمكنك استخدام بيانات اعتماد المستخدم الخاصة بتطبيق .ABC ثم يطلب XYZ رمز الوصول من ABC بالنيابة عنك. والآن يتاح لك الوصول إلى XYZ .

XYZلا يعرف أي شيء عنك أو عن بيانات اعتماد الاستخدام الخاصة بك، لذلك فهذا الاتصال لا يوجد اشتباه. استخدام الرموز المميزة السرية يمنع التطبيقات الضارة من الحصول على معلوماتك وبياناتك.

لا تقم بمشاركة الكثير من معلوماتك على مواقع التواصل الاجتماعي

إذا كنت ترغب في الاحتفاظ بالخصوصية على مواقع التواصل الاجتماعي، فشارك المعلومات بأقل قدر ممكن. ولا يجب مشاركة معلومات مثل تاريخ الميلاد أو عنوان البريد الإلكتروني أو رقم الهاتف على صفحتك الشخصية. فالأشخاص الذين يحتاجون إلى معرفة معلوماتك الشخصية، من المحتمل أنهم يعرفونها بالفعل. ولا تقم بملء صفحتك الشخصية تمامًا على الوسائط الاجتماعية، بل قم بالمشاركة بالحد الأدنى من المعلومات المطلوبة فقط. علاوة على ذلك، تحقق من إعدادات مواقع التواصل الاجتماعي للسماح للأشخاص الذين تعرفهم فقط برؤية أنشطتك أو الاشتراك في المحادثة.

وكلما زادت المعلومات الشخصية التي تشاركها عبر الإنترنت، كلما سهل على الأشخاص إنشاء صفحة شخصية عنك واستغلالك عندما لا تكون متصلًا.

هل سبق ونسيت اسم المستخدم وكلمة المرور لحساب عبر إنترنت؟ الأسئلة المتعلقة بالأمان مثل "ما هو اسم الأم قبل الزواج؟" أو "في أي مدينة ولدت؟" من المفترض أن تساعد على الحفاظ على الأمن ضد المتسللين لحسابك. ومع ذلك، فإن أي شخص يرغب في الوصول إلى حساباتك، يمكنه البحث عن الإجابات على الإنترنت. يمكنك الرد على هذه الأسئلة بمعلومات خاطئة، طالما تتذكر الإجابات خطأ. إذا كان لديك مشكلة في تذكرها، يمكنك استخدام برنامج لإدارة كلمات المرور لإدارتها بالنيابة عنك.

خصوصية مستعرض الويب والبريد الإلكتروني

يوميًا، يتم إرسال الملايين من رسائل البريد الإلكتروني للتواصل مع الأصدقاء وإدارة الأعمال. فالبريد الإلكتروني يعدّ طريقة مريحة للاتصال السريع بين الأشخاص. عندما ترسل رسالة بريد إلكتروني، يكون الأمر مشابهاً لإرسال رسالة باستخدام البطاقة البريدية. يتم نقل رسالة البطاقة البريدية على مرئى ممن لديه إمكانية الاطلاع، كما يتم إرسالها بالنص العادي وهو أيضًا على مرئى ممن لديه إمكانية الوصول. كما يتم تمرير هذه الاتصالات بين أجهزة خوادم المختلفة وهي في مسارها إلى الوجهة. وحتى مع حذف رسائل بريد الإلكتروني، قد يتم أرشفة الرسائل على أجهزة خوادم البريد لبعض الوقت.

يستطيع أي شخص لديه إمكانية الوصول المادي إلى حاسوبك، أو جهاز التوجيه، الاطلاع على مواقع الويب التي قمت بزيارتها من خلال محفوظات مستعرض الويب وذاكرة التخزين المؤقت وربما ملفات السجل. يمكن تقليل حجم هذه المشكلة من خلال استخدام وضع الاستعراض الخاص في متصفح الويب. تشتمل معظم متصفحات الويب الشائعة على اسم خاص بها يمثل وضع المستعرض الخاص:

- **Microsoft Internet Explorer**: InPrivate
- **Google Chrome**: Incognito
- **Mozilla Firefox**: Private tab / private window
- **Safari**: Private: Private browsing

مع استخدام وضع التصفح الخاص، تتعطل ملفات تعريف الارتباط، ويتم إزالة ملفات الإنترنت المؤقتة ومحفوظات التصفح بعد غلق النافذة أو البرنامج.

الاحتفاظ بخصوصية محفوظات تصفح الإنترنت قد يمنع الآخرين من جمع المعلومات حول أنشطتك عبر الإنترنت وإغراءك بشراء شيء باستخدام الإعلانات الموجهة. حتى مع استخدام التصفح الخاص وتعطيل ملفات تعريف الارتباط، تطور الشركات المختلفة طرقاً متنوعة للتعرف على اهتمامات المستخدمين لجمع المعلومات وتتبع السلوك. على سبيل المثال، يمكن أن تحتوي الأجهزة الوسيطة، مثل أجهزة التوجيه، معلومات حول محفوظات تصفح الويب الخاصة بالمستخدم.

في النهاية، فإن مسؤليتك هي حماية بياناتك وهويتك وأجهزة الحوسبة. هل تحتاج إلى إرفاق السجلات الطبية الخاصة بك عندما ترسل رسالة بريد إلكتروني؟ تأكد من أمن عملية الإرسال، عندما تتصفح الإنترنت في المرة القادمة. القليل من الاحتياطات البسيطة قد تمنع حدوث المشاكل لاحقًا.

الفصل الثالث: حماية بياناتك وخصوصيتك

لقد ركز هذا الفصل على الأجهزة الشخصية والبيانات الشخصية. واشتمل على النصائح لحماية الأجهزة وإنشاء كلمات المرور القوية واستخدام الشبكات اللاسلكية بأمان. وتناول كذلك النسخ الاحتياطي للبيانات وتخزين البيانات وحذف البيانات نهائياً.

وتمت مناقشة أساليب المصادقة للمساعدة في الحفاظ على أمن البيانات. وتناول بإيجاز مدى سهولة المشاركة للكثير من المعلومات على مواقع التواصل الاجتماعي وكيفية تجنب تلك الخطورة الأمنية.

الفصل الرابع: حماية المنظمة

يتناول هذا الفصل بعض التقنيات والعمليات المستخدمة بواسطة محترفي الأمن السيبراني عند حماية شبكات المؤسسات وأجهزتها وبياناتها. أولاً، يتناول بإيجاز الأنواع العديدة من جدران الحماية، وأجهزة الأمان والبرامج المستخدمة حاليا، بما في ذلك أفضل الممارسات.

وبعد ذلك، يشرح هذا الفصل أجهزة روبوت الشبكات وسلسلة الهجوم والأمان المبني على السلوك، واستخدام NetFlow لمراقبة الشبكات.

يناقش القسم الثالث نهج شركة Cisco المتعلق بالأمن السيبراني، بما في ذلك فريق الاستجابة للحوادث الأمنية (CSIRT) ودليل الإرشادات الأمنية. ويتناول بإيجاز الأدوات التي يستخدمها محترفو الأمن السيبراني لكشف هجمات الشبكة ومنعها.

أنواع جدران الحماية

جدار الحماية هو عبارة عن جدار أو قسم مصمم لمنع الحريق من الانتشار من أحد أجزاء المبنى إلى الأجزاء الأخرى. في مجال شبكات الحاسوب، يتم تصميم جدار الحماية للتحكم في تحديد ما هي الاتصالات التي يمكن السماح لها بالمرور إلى الأجهزة أو الشبكات وما هي الاتصالات التي يمكن السماح لها بالخروج. يمكن تثبيت جدار الحماية على جهاز حاسوب واحد بغرض حمايته (جدار حماية مستند إلى جهاز المستخدم)، أو يمكن أن يكون جهازًا بشبكة مستقلة يحمي شبكة كاملة من أجهزة الحاسوب وجميع الأجهزة المضيفة على تلك الشبكة (جدار حماية مستند إلى الشبكة).

على مدار السنوات، كلما أصبحت أجهزة الحاسوب والهجمات على الشبكة أكثر تعقيداً كلما ظهرت أنواع جديدة من جدران الحماية المُطَورة التي لها أغراضاً مختلفة في حماية شبكة. فيما يلي قائمة بأنواع جدران الحماية الشائعة:

- **جدار حماية طبقة الشبكة** حيث التصفية بناءً على عناوين IP للمصدر والوجهة
- **جدار حماية طبقة النقل** حيث التصفية بناءً على منافذ البيانات للمصدر والوجهة، والتصفية بناءً على حالات الاتصال
- **جدار حماية طبقة التطبيق** حيث التصفية بناءً على التطبيق أو البرنامج أو الخدمة
- **جدار حماية التطبيق بالنسبة للسياق** حيث التصفية بناءً على المستخدم والجهاز والدور ونوع التطبيق وخصائص التهديدات
- **جهاز خادم الوكيل** حيث تكون التصفية لطلبات محتوى الويب كعنوان URL أو المجال أو الوسائط، إلخ.

- **جهاز خادم الوكيل العكسي** يوضع أمام أجهزة خوادم الويب، وتقوم أجهزة خوادم الوكيل العكسية بحماية الوصول إلى أجهزة خوادم الويب وإخفاءه وتوزيعه والغاء تحميله
- **جدران الحماية لنقل عناوين الشبكات (NAT)** تخفي العناوين الخاصة بأجهزة الشبكة
- **جدران الحماية المستندة إلى جهاز المستخدم** -تصفية المنافذ وطلبات خدمة النظام على نظام تشغيل حاسوبي واحد

فحص المنافذ

فحص المنفذ هي عملية التدقيق في أجهزة الحاسوب أو أجهزة الخوادم أو مضيفات الشبكات الأخرى للمنافذ المفتوحة. في مجال الشبكات، يتم تعيين معرف يسمى رقم المنفذ لكل التطبيقات التي تعمل على الأجهزة. يتم استخدام هذا الرقم في كلا طرفي الإرسال حيث يتم تمرير البيانات الصحيحة إلى التطبيق الصحيح. يمكن استخدام فحص المنفذ بشكل ضار كأداة استطلاع للتعرف على أنظمة التشغيل والخدمات التي تعمل على أجهزة الحاسوب أو أجهزة جهاز المضيفات، أو يمكن استخدامه بلا ضرر عن طريق مسؤول الشبكات للتحقق من سياسات أمان الشبكة.

لأغراض تقييم أمان المنفذ وجدار الحماية لشبكة الحاسوب، يمكنك استخدام أداة لفحص المنفذ مثل Nmapللبحث عن جميع المنافذ المفتوحة في الشبكة. ويمكن اعتبار عملية فحص المنفذ بأنها منذرة بالهجمات التي تتعرّض لها الشبكة وبالتالي يجب عدم القيام بها على الأجهزة خوادم العامة على الإنترنت، أو على شبكة الشركة دون إذن.

لتنفيذ عملية فحص Nmap للمنفذ في جهاز الحاسوب على شبكة الاتصال المحلية، قم بتنزيل برنامج مثل Zenmap وابدأ تشغيله، ثم اكتب عنوان IP لجهاز الحاسوب المستهدف المراد فحصه واختر افتراضية فحص ملف التعريف واضغط على فحص. وسيقوم فحص Nmap بالإبلاغ عن جميع الخدمات قيد التشغيل (على سبيل المثال، خدمات الويب أو خدمات البريد، إلخ) وأرقام المنافذ. وتتمثل نتائج فحص المنافذ بشكل عام في واحدة من تلك الاستجابات الثلاثة:

- **مفتوحة أو مقبولة** قام جهاز المضيف بالرد مما يشير إلى ترقب الخدمة على المنفذ.
- **مغلقة أو مرفوضة أو غير مترقبة** تشير إلى رفض جهاز المضيف للاتصالات بالمنفذ.
- **مصفاة أو مسقطة أو محظورة** لم يرد جهاز المضيف.

لإجراء فحوصات المنفذ للشبكة من خارج الشبكة، فستحتاج إلى بدء الفحص من خارج الشبكة. ويشمل ذلك تشغيل فحص المنفذ من خلال Nmap مقابل جدار الحماية أو عنوان IP العام للموجه. لاكتشاف عنوان IP العام الخاص بك، استخدم محرك بحث مثل Google بالاستعلام "ما هو عنوان ipالخاص بي". وسيقوم محرك البحث بإظهار عنوان IP العام الخاص بك.

لتشغيل عمليات فحص المنافذ لستة منافذ شائعة مقابل الموجه المنزلي أو جدار الحماية، انتقل إلى فحص المنافذ من خلال Nmap عبر الإنترنت على موقع الويب https://hackertarget.com/nmap-online-port-scanner/ وأدخل عنوان IP العام الخاص بك في مربع الإدخال *IP address : to scan...* واضغط على *Quick Nmap Scan.* إذا كانت الاستجابة *open* لكل من المنافذ التالية:٢١ أو ٢٢ أو ٢٥ أو ٨٠ أو ٤٤٣ أو ٣٣٨٩ فغالبًا، قد تم تمكين إعادة توجيه المنفذ في الموجه أو جدار الحماية، بالإضافة إلى أنك تقوم بتشغيل الأجهزة خوادم على الشبكة الخاصة بك.

الأجهزة الأمنية

اليوم لا توجد أجهزة أمان منفردة أو تقنية من التقنيات يمكنها تلبية جميع الاحتياجات الأمنية للشبكة، ونظراً لوجود مجموعة متنوعة من أجهزة الأمان والأدوات التي تحتاج إلى تنفيذها، فمن المهم أن تعمل معًا جميع الأجهزة والأدوات. وتصبح أجهزة الأمان أكثر تأثيراً عندما تكون جزءً من النظام.

يمكن أن تكون أجهزة الأمان مستقلة، مثل أجهزة التوجيه أو جدران الحماية أو البطاقات التي يمكن تثبيتها في الاجهزة القابلة للاتصال بالشبكة أو الوحدات المجهزة بالمعالجات وذاكرات التخزين المؤقت. يمكن أن تكون أجهزة الأمان أدوات برمجية يتم تشغيلها على الأجهزة القابلة للاتصال بالشبكة. تندرج الأجهزة الأمنية في هذه الفئات العامة:

أجهزة التوجيه وتشمل موجهات(ISR) Cisco Integrated Services Router ، وتتميز بالعديد من قدرات جدران الحماية بالإضافة إلى وظائف التوجيه، بما في ذلك تصفية نقل البيانات والقدرة على تشغيل (IPS) Intrusion Prevention System والتشفير وقدرات شبكات VPN للحصول على عملية توصيل آمنة ومشفرة.

جدران الحماية -تحتوي جدران الحماية من الجيل التالي من Cisco على كافة قدرات الموجه ISR، بالإضافة إلى التحليلات والإدارة المتقدمة للشبكة.

- **IPS** أجهزة Cisco IPS من الجيل التالي، مخصصة لمنع الاختراق.

- **VPN** أجهزة Cisco للأمان مزودة بتقنيات أجهزة خوادم الشبكات الخاصة الافتراضية (VPN) وعملائها. وهي مصممة لعملية النقل المشفرة والآمنة.

البرامج الضارة وبرامج الحماية من الفيروسات -الحماية المتقدمة من البرامج الضارة من شركة Cisco (AMP) مضمنة في الجيل التالي من موجهات Cisco وجدران الحماية وأجهزة IPS وأجهزة الويب وأمن البريد الإلكتروني ويمكن أيضًا تثبيتها كبرامج في أجهزة الحاسوب جهاز المضيفة.

تتضمن فئة **أجهزة الأمان أخرى** أجهزة الأمان للويب والبريد الإلكتروني وأجهزة فك التشفير وأجهزة خوادم التحكم بوصول العميل وأنظمة إدارة الأمان.

اكتشاف الهجمات في الوقت الفعلي

لا توجد برامج مثالية. وعندما يستغل المتسللون الخلل في جزء من البرنامج قبل أن يصلحه المطور، فإن هذا يعرف بهجمة اليوم الأول. ونظراً لتطور هجمات اليوم الأول وضخامتها حاليًا، فقد أصبح من الشائع نجاح الهجمات على الشبكة كما أصبح التصدي لتلك الهجمات يقاس بمدى سرعة استجابة الشبكة لها. ويكمن الهدف المثالي في القدرة على اكتشاف الهجمات عند حدوثها في الوقت الفعلي، وإيقافها على الفور، أو في خلال دقائق من حدوثها. ولسوء الحظ، فالعديد من الشركات والمؤسسات لا يمكنها اكتشاف الهجمات إلا بعد أيام أو حتى شهور من وقت حدوثها.

- **الفحص في الوقت الفعلي من البداية إلى النهاية** يتطلب اكتشاف الهجمات في الوقت الفعلي الفحص المستمر للبحث عن الهجمات باستخدام جدران الحماية والأجهزة القابلة للاتصال بالشبكة من خلالIDS أو .IPS يجب استخدام أجهزة الجيل التالي للعميل أو الخادم لاكتشاف البرامج الضارة المتصلة بمراكز التهديد العالمية عبر الإنترنت. حاليًا، يمكن لأجهزة المسح النشطة وبرامجها كشف حدوث الأخطاء في الشبكة باستخدام كشف السلوكيات والتحليل المبني على السياق.
- **هجمات DDoS والاستجابة الفعلية** هجمات DDoS هي واحدة من أقوى التهديدات الهجومية التي تتطلب الاستجابة والكشف في الوقت الفعلي. ويعتبر التصدي لهجمات DDoS أمرًا بالغ الصعوبة لأن تلك الهجمات تنشأ من المئات أو الآلاف من الأجهزة جهاز المضيفة المُستغَلة وتظهر في شكل حركة نقل للبيانات موثوق بها، كما هو موضح في الشكل. وبالنسبة للشركات والمؤسسات، فإن هجمات DDoS التي تحدث بانتظام تصيب الأجهزة خوادم على الإنترنت وتؤثر على توفر الشبكة. والقدرة على كشف هجمات DDoS والتصدي لها هو أمر حتمي.

الحماية من البرامج الضارة

كيف يمكنك التصدي لهجمات اليوم الأول وكذلك التهديدات المتقدمة المستمرة (APT) التي تسرق البيانات لفترة طويلة؟ من ضمن الحلول، استخدام برنامج على مستوى الشركات متكامل ومتقدم للكشف عن البرامج الضارة بحيث يتميز بكشفها في الوقت الفعلي.

ويتحتم على المسئولين عن الشبكة المراقبة المستمرة للشبكة لاكتشاف العلامات الدالة على وجود البرامج الضارة أو السلوكيات التي تنبئ عن وجود APT. تمتلك شركة Cisco الحماية المتقدمة من البرامج الضارة (AMP) وهي شبكة تهديدات تحلل الملايين من الملفات وتقارنها بمئات الملايين من نتائج تحليل البرامج الضارة الأخرى. وهذا يوفر نظرة شاملة على هجمات البرامج الضارة والحملات وتوزيعها. AMP هو برنامج للعميل أو الجهاز الخادم ينتشر في نهايات أجهزة جهاز المضيفات كجهاز خادم مستقل أو على أجهزة أمن الشبكات الأخرى.

أفضل ممارسات الأمان

قامت العديد من المؤسسات الدولية والمهنية بنشر قوائم بأفضل الممارسات الأمنية. فيما يلي قائمة ببعض أفضل الممارسات الأمنية:

- **إجراء تقييم المخاطر** -إن معرفة قيمة ما تقوم بحمايته سيساعد في تبرير النفقات الأمنية.
- **إنشاء سياسة أمان** -أنشئ سياسة تحدد قواعد الشركة وواجباتها وتوقعاتها بوضوح.
- **تدابير الأمن المادية** -تقييد الوصول إلى حجرات الشبكات ومواقع الجهاز الخادم فضلا عن التصدي للهجمات.
- **تدابير أمن الموارد البشرية** -يجب أن يتم بحث الموظفين بشكل صحيح من خلال إجراء الاختبارات لتحديد مهارتهم.
- **أداء واختبار النسخ الاحتياطية** -إجراء نسخ احتياطي منتظم واختبار استعادة البيانات من النسخ الاحتياطية.
- **المداومة على إجراء تصحيحات الأمان والتحديثات** -قم بتحديث أنظمة وبرامج تشغيل الأجهزة والعميل والشبكة بشكل منتظم.
- **توظيف ضوابط الوصول** -تكوين أدوار المستخدم ومستويات الامتيازات بالإضافة إلى مصادقة المستخدم القوية.
- **اختبار الاستجابة للحوادث بانتظام** -توظيف فريق الاستجابة للحوادث واختبار سيناريوهات الاستجابة للطوارئ.
- **توظيف أدوات مراقبة الشبكة والتحليلات والأدوات الإدارية** -اختر حل مراقبة الأمان الذي يتكامل مع التقنيات الأخرى.

- **توظيف أجهزة أمن الشبكات** -استخدم أجهزة توجيه الجيل التالي وجدران الحماية وأجهزة الأمان الأخرى.
- **تنفيذ حل شامل لأمن النقاط الطرفية** -استخدام برامج مكافحة البرامج الضارة على مستوى المؤسسة وبرامج الحماية من الفيروسات.
- **تثقيف المستخدمين** -تثقيف المستخدمين والموظفين بالإجراءات الآمنة.
- **تشفير البيانات** -تشفير جميع بيانات الشركة الحساسة بما في ذلك رسائل البريد الإلكتروني.

وتوجد بعض الإرشادات الأكثر إفادة في المستودعات التنظيمية مثل المعهد الوطني للمعايير والتكنولوجيا (NIST) مركز الموارد الأمنية لأجهزة الحاسوب، كما هو موضح في الشكل.

ويعتبر معهد SANS من أكثر المؤسسات شهرة وتبجيلًا على نطاق واسع يقوم بالتدريب على الأمن السيبراني.

روبوت الشبكة

روبوت الشبكة هو عبارة عن مجموعة من أجهزة الروبوت المتصلة عبر الإنترنت، يمكن للأشخاص أو المجموعات الضارة التحكم بها. ويصاب الحاسوب الروبوت غالبًا عند زيارة مواقع الويب أو فتح مرفقات البريد إلكتروني أو فتح ملفات وسائط مصابة.

ويمكن أن يمتلك روبوت الشبكات عشرات الآلاف أو مئات الآلاف من الروبوت. يمكن تنشيط أجهزة الروبوت لتوزيع البرامج الضارة أو شن هجمات DDoS أو توزيع البريد الإلكتروني العشوائي أو شن هجمات القوة الغاشمة بكلمات المرور. وعادة ما يتم التحكم في روبوت الشبكات من خلال جهاز خادم القيادة والسيطرة.

يقوم المجرمون الإلكترونيون بتأجير أجهزة روبوت الشبكات، مقابل رسوم لأطراف ثالثة لأغراض شريرة.

يوضح هذا الشكل كيفية استخدام تصفية حركة بيانات أجهزة روبوت الشبكات لإعلام المجتمع الأمني في جميع أنحاء العالم بمواقعها.

سلسلة الهجوم في الدفاع الإلكتروني

في مجال الأمن السيبراني، سلسلة الهجوم هي مراحل الهجوم على أنظمة المعلومات. طور Lockheed Martin سلسلة الهجوم كنظام أمني للكشف عن الحوادث والاستجابة لها، وهي تتكون من المراحل التالية:

المرحلة الأولى. الاستطلاع حيث يقوم المهاجم بجمع المعلومات حول الهدف.

المرحلة الثانية. التسليح حيث يقوم المهاجم بتكوين العمليات الاستغلالية وحاملات الضرر حتى يرسلها إلى الهدف.

المرحلة الثالثة. التوصيل حيث يرسل المهاجم العمليات الاستغلالية وحاملات الضرر إلى الهدف على البريد الإلكتروني أو بطرق أخرى.

المرحلة الرابعة. الاستغلال حيث يتم تنفيذ العمليات الاستغلالية.

المرحلة الخامسة التثبيت حيث يتم تثبيت البرامج الضارة وبرامج المراقبة على الهدف.

المرحلة السادسة. القيادة والسيطرة حيث يتم اكتساب عملية التحكم في الهدف عن بعد من خلال قنوات أو أجهزة خوادم القيادة والسيطرة.

المرحلة السابعة. الإجراءات حيث يمكن للمهاجم تنفيذ الإجراءات الضارة مثل سرقة المعلومات أو تنفيذ هجمات إضافية على أجهزة أخرى من داخل الشبكة عن طريق العمل من خلال مراحل سلسلة الهجوم مرة أخرى.

للتصدي لسلسلة الهجوم، تم تصميم دفاعات أمان الشبكة بالاقتباس من مراحل سلسلة الهجوم. وفيما يلي بعض الأسئلة حول دفاعات الأمان للشركة، بناءً على سلسلة الهجوم الإلكتروني:

• ما هي المؤشرات على حدوث الهجمات في كل مرحلة من مراحل سلسلة الهجوم؟

•وما هي أدوات الأمان اللازمة للكشف عن مؤشرات الهجوم في كل مرحلة من المراحل؟

•هل توجد ثغرات في قدرة الشركة على الكشف عن الهجمات؟

وكما وضحLockheed Martin، بأن فهم مراحل سلسلة الهجوم يسمح لهم بوضع عقبات دفاعية وإبطاء الهجمات ومنع فقدان البيانات في النهاية. يوضح هذا الشكل كيف أن كل مرحلة من مراحل سلسلة الهجوم تعادل الزيادة في مقدار الجهد والتكلفة لمنع الهجمات واحتواءها.

الأمان المبني على السلوك

الأمان المبني على السلوك هو أحد أشكال اكتشاف التهديدات الذي لا يعتمد على التوقيعات الضارة المعروفة، بل يستخدم السياق للكشف عن حدوث أخطاء في الشبكة. ويتضمن الأمان المبني على السلوك التقاط تدفق الاتصال بين المستخدمين على الشبكات المحلية وبين الوجهات المحلية أو البعيدة وتحليله. وعند التقاط تلك الاتصالات وتحليلها، تتبين السياقات وأنماط السلوك التي يمكن استخدامها للكشف عن حدوث أخطاء. والكشف المبني على السلوك يمكنه اكتشاف وجود الهجمات من خلال التغير في السلوك الطبيعي.

- **المصايد** هي أداة من أدوات الكشف المبني على السلوك التي تغري المهاجم في البداية من خلال مجاراة الأنماط المتوقعة في سلوك المهاجم الضار، وعند دخول المصيدة، يمكن للمسؤول عن الشبكة التقاط سلوك المهاجم وتسجيله وتحليله. وهذا يسمح للمسؤول بالحصول على مزيد من المعرفة وبناء دفاع أفضل.

- **بنية حلول التصدي للتهديدات الإلكترونية من cisco** هي بنية أمان تستخدم الكشف المبني على السلوك بالإضافة إلى المؤشرات، لتوفير الرؤية والسياق والتحكم بشكل أكبر. ويكمن الهدف في معرفة من يقوم بالهجوم وأين ومتى وكيف. وتستخدم هذه البنية الأمنية العديد من تقنيات الأمان لتحقيق هذا الهدف.

NetFlow

يتم استخدام تقنية NetFlow لجمع المعلومات حول تدفق البيانات عبر شبكة. ويمكن تشبيه معلومات NetFlowبفاتورة الهاتف لحركة بيانات الشبكة. حيث تقوم بإظهار الأشخاص والأجهزة الموجودة على شبكتك، بالإضافة إلى زمان ومكان وكيفية وصول المستخدمين إليها NetFlow .هو مكون مهم في عملية الكشف المبني على السلوك وتحليله. يمكن للمحولات وأجهزة التوجيه وجدران الحماية المزودة بتقنية NetFlow الإبلاغ بالمعلومات حول الدخول على البيانات والخروج والتنقل عبر الشبكة. ويتم إرسال المعلومات إلى أدوات تجميع NetFlow التي تجمع سجلات NetFlow وتخزنها وتحللها.

ويمتلك NetFlow القدرة على تجميع المعلومات حول الاستخدام من خلال العديد من الخصائص المختلفة لكيفية نقل البيانات عبر الشبكة، كما هو موضح في الشكل. وعن طريق جمع المعلومات حول تدفق بيانات الشبكة، يصبح NetFlow قادرًا على إنشاء السلوكيات الأساسية لأكثر من ٩٠ سمة مختلفة.

CSIRT

تحتوي العديد من المؤسسات الكبيرة على فرق الاستجابة لحوادث الأمان على أجهزة الحاسوب (CSIRT) لاستقبال البلاغات الخاصة بأمان أجهزة الحاسوب ومراجعتها والرد عليها، وتعتبر مهمة CSIRTالأساسية هي المساعدة في ضمان الحفاظ على الشركة وأنظمتها وبياناتها عن طريق إجراء التحريات الشاملة عن حوادث الأمان على أجهزة الحاسوب. ولمنع الحوادث الأمنية، توفر Cisco CSIRT المساعدة الاستباقية حول التهديدات وخطط تخفيف أثرها، وتحليل إتجاهات الحوادث ومراجعة بنية الأمان.

تتعاون فرق CSIRT في شركة Cisco مع منتدى الاستجابة للحوادث وفرق الأمن (FIRST) وتبادل معلومات السلامة الوطنية (NSIE) وتبادل معلومات الأمن الدفاعي (DSIE) ومركز تحليل وبحث عملياتDNS (DNS-OARC)

هناك منظمات CSIRT وطنية وعامة مثل قسمCERT في معهد هندسة البرمجيات بجامعة Carnegie Mellon، والتي تتوفر لمساعدة المنظمات وفرق CSIRT الوطنية في تطوير قدراتهم على إدارة الحوادث وفي التعامل معها وتحسينها.

تتغير التكنولوجيا باستمرار، مما يعني أن الهجمات الأمنية تتطور أيضًا. ويتم اكتشاف الثغرات الأمنية الجديدة وأساليب الهجوم باستمرار. وأصبح الأمن مصدر قلق كبير في مجال الأعمال نظراً لتأثير الاختراقات الأمنية على سمعة الشركات والأموال. وتقوم الهجمات باستهداف الشبكات المهمة والبيانات الحساسة. ويتحتم على المنظمات عمل الخطط للاستعداد للاختراقات والتعامل معها والتخلص من أثرها.

ومنع الاختراقات الأمنية هي من أفضل طرق للاستعداد لها. يجب أن تتوفر الإرشادات للتعريف بمخاطر الأمن السيبراني على الأنظمة، والأصول والبيانات والقدرات، وحماية النظام عن طريق تنفيذ الإجراءات الوقائية وتدريب الموظفين، والكشف عن حوادث الأمن السيبراني بأسرع وقت ممكن. وعند الكشف عن اختراقات الأمان، يجب اتخاذ الإجراءات المناسبة لتقليل أثرها وضررها. يجب أن تكون خطة الاستجابة مرنة ومجهزة بعدة خيارات للإجراءات اللازمة خلال الاخترقات. وبعد احتواء الاختراق واستعادة الأنظمة والخدمات المهددة، يجب تحديث التدابير والعمليات الأمنية لتشمل الدروس المستفادة أثناء حدوث هذا الاختراق.

ويجب تجميع هذه المعلومات بأكملها في كتاب الإرشادات الامنية. كتاب الإرشادات الأمنية هو مجموعة من استعلامات قابلة للتكرار (التقارير) عن مصادر بيانات حوادث الأمان التي تؤدي إلى الكشف عن الحوادث والاستجابة لها. وبشكل مثالي يجب أن تتوفر الإجراءات التالية في كتاب الإرشادات الأمنية:

- كشف الأجهزة المصابة بالبرامج الضارة
- كشف الأنشطة المشبوهة في الشبكة.
- الكشف عن محاولات التوثيق غير النظامية.
- وصف وفهم حركة نقل البيانات الواردة والصادرة.
- توفير المعلومات التلخيصية بما في ذلك المؤشرات والإحصاءات والأعداد.
- توفير وصول سهل وسريع إلى الإحصاءات والمقاييس.
- ربط الأحداث عبر جميع مصادر البيانات المتعلقة.

أدوات لمنع الحوادث وكشفها

فيما يلي بعض الأدوات المستخدمة لكشف الحوادث الأمنية ومنعها:

- **SIEM** معلومات الأمان ونظام إدارة الحوادث (SIEM) هو برنامج يجمع ويحلل تنبيهات الأمان والسجلات، والبيانات المستجدة والتاريخية، من أجهزة الأمان على الشبكة.

- **DLP** برامج منع فقد البيانات (DLP) هو نظام برمجي أو مادي مصمم لمنع سرقة البيانات الحساسة أو تسربها من الشبكات. وقد يهتم نظام DLP بعملية ترخيص الوصول إلى الملفات وتبادل البيانات ونسخها، ومراقبة نشاط المستخدم والمزيد. تم تصميم أنظمة DLP لمراقبة وحماية البيانات في ثلاث حالات مختلفة: البيانات قيد الاستخدام والبيانات المتحركة والبيانات المستقرة. وتركز البيانات قيد الاستخدام على العميل، وتشير البيانات المتحركة إلى البيانات التي تتحرك داخل الشبكة، كما تشير البيانات المستقرة إلى عملية تخزين البيانات.

- **ISEو TrustSec من Cisco** ترغم Cisco Identity Services Engine (Cisco ISE) و Cisco TrustSec الوصول إلى مصادر الشبكات من خلال إنشاء سياسات تحكم في الوصول مبنية على الأدوار التي تقسم الوصول إلى الشبكة (الضيوف ومستخدمي الهاتف المحمول والموظفين) دون إضافة التعقيدات. ويعتمد تصنيف حركة البيانات على هوية المستخدم أو الجهاز.

IDSوIPS

نظام كشف الاقتحام(IDS) ، الموضح في الشكل، هو إما جهاز مخصص للشبكات، أو أداة واحدة ضمن العديد من الأدوات في الأجهزة خوادم أو جدران الحماية التي تعمل على فحص البيانات لقواعد البيانات أو توقيعات الهجوم، لكي تبحث عن حركات البيانات الضارة. في حالة اكتشاف تطابق، سيقوم IDS بتسجيل الاكتشاف، ثم تنبيه مسؤول الشبكات. لا يقوم نظام الكشف عن الاقتحام باتخاذ الإجراءات عند اكتشاف المطابقات، وبالتالي فهو لا يمنع حدوث الهجمات. وتكمن وظيفة IDSفقط في الكشف والتسجيل والتقرير.

أما الفحوصات التي يجريها IDS فهي تبطئ من سرعة الشبكة (ويعرف ذلك بوقت الاستجابة). لمنع تعطيل الشبكة، يوضع IDS للعمل دون اتصال ومنفصل عن حركة بيانات الشبكة العادية. يتم نسخ البيانات أو إجراء نسخ متطابق لها بمحول ثم إعادة توجيهها إلى IDS لإجراء الكشف دون اتصال. توجد أيضا أدوات IDS يمكن تثبيتها على نظام التشغيل الخاص بجهاز حاسوب جهاز المضيف، مثل WindowsأوLinux.

نظام الوقاية من الاقتحام (IPS) لديه القدرة على حظر حركة البيانات أو رفضها استناداً إلى قاعدة إيجابية أو مطابقة التوقيع. ويعتبر Snort من أشهر أنظمة IPS/IDS. والإصدار التجاري من Snort هو Sourcefire من شركة Cisco. كما أن Sourcefire لديه القدرة على تنفيذ حركة البيانات في الوقت الفعلي وتحليل المنافذ وإنشاء السجلات، والبحث عن المحتوى ومطابقته، واكتشاف الهجمات وبرامج الاستطلاع، وفحص المنافذ. ويتكامل أيضا مع الأدوات الخارجية الأخرى للإبلاغ وتحليل الأداء والسجلات..

الفصل الرابع: حماية المنظمة

بدأ هذا الفصل بمناقشة بعض التقنيات والعمليات التي يستخدمها محترفو الأمن السيبراني عند حماية شبكات المؤسسات وأجهزتها وبياناتها. وتشمل أنواع جدران الحماية، وأجهزة الأمان والبرامج.

وتم تناول استخدام NetFlow لمراقبة الشبكات وأجهزة روبوت الشبكات وسلسلة الهجوم والأمان المبني على السلوك.

وأخيراً، تم توضيح نهج Cisco فيما يخص الأمن السيبراني، بما في ذلك فرق CSIRT وتم شرح دليل الإرشادات الأمنية. وهو يتناول بإيجاز الأدوات التي يستخدمها محترفو الأمن السيبراني لكشف الهجمات على الشبكة ومنعها، بما في ذلك SIEM و DLP و Cisco ISE وTrustSec ، بالإضافة إلى أنظمة IDS و.IPS

الفصل الخامس: هل سيكون مستقبلك في مجال الأمن السيبراني

يتناول هذا الفصل المشكلات الأخلاقية والقانونية الناتجة عن العمل في مجال الأمن السيبراني. كما يتناول أيضا المسار التعليمي والمهني لمجال الأمن السيبراني. وتوجد المسارات التعليمية ذات الشهادات التي قد ترغب في الالتحاق بها من .Cisco Networking Academy وبعض هذه الشهادات يعتبر من المتطلبات الأساسية لشهادات التخصص في العديد من مجالات الشبكات، بما في ذلك الأمن السيبراني.

توفر صفحة برنامج التوظيف (Networking Academy Talent Bridge لقاء المواهب في أكاديمية الشبكات netacad.com) (تحت قائمة الموارد) معلومات جيدة لمساعدتك في كتابة السيرة الذاتية المميزة والتحضير لإجراء مقابلات العمل. كما يحتوي على قوائم بالوظائف داخل Cisco وشركائها. يتم تقديم ثلاثة محركات بحث خارجية مهمة لوظائف الإنترنت لاستكشافها.

المشكلات القانونية في مجال الأمن السيبراني

يتحتم على محترفي الأمن السيبراني امتلاك المهارات بنفس قدر المهاجمين، خاصةً المهاجمين لأغراض ضارة، من أجل التصدي للهجمات. والاختلاف الوحيد بين المهاجم ومحترف الأمن السيبراني هو أن الثاني يجب عليه العمل في سياق قانوني.

الأمور القانونية الشخصية

ولا تحتاج أن تكون موظفًا حتى تُطبق عليك قوانين الأمن السيبراني ففي الحياة الشخصية، قد تمتلك الفرصة والمهارات لاختراق أجهزة الحاسوب أو الشبكات الخاصة بأشخاص الآخرين. وهناك مقولة "امتلاك القدرة على فعل شيء لا يعني وجوب فعله". ضع ذلك في الاعتبار. يترك معظم المتسللين المسارات، التي يمكن تتبعها حتى الوصول لهم، سواء كانوا يعلمون ذلك أم لا.

ويعمل محترفو الأمن السيبراني على إصقال العديد من المهارات التي يمكن استخدامها في خدمة الخير أو الشر. والأشخاص الذين يستخدمون مهاراتهم في نطاق السياقات القانونية، لحماية البنى الأساسية والشبكات والخصوصيات مطلوبون للعمل بكثرة دائمًا.

الأمور القانونية للشركات

معظم الدول لديها بعض القوانين المتعلقة بالأمن السيبراني. وقد تحتاج إلى تنفيذها مع البنى الأساسية المهمة والشبكات، والخصوصيات المشتركة والفردية. ويتحتم على الشركات الالتزام بتلك القوانين.

في بعض الحالات، إذا قمت بخرق قوانين الأمن السيبراني أثناء القيام بالعمل، فإن العقاب قد يقع على الشركة وبالتالي قد تخسر وظيفتك. في حالات أخرى، قد يؤدي ذلك إلى محاكمتك أو تغريمك أو ربما الحكم عليك.

وبوجه عام، إذا اختلطت عليك الأمور ولم تكن متأكدًا من قانونية بعض الإجراءات أو السلوكيات، فافترض بأنها غير قانونية ولا تفعلها. وقد تحتوي الشركة على قسم متعلق بالشئون القانونية، أو قد تجد في قسم الموارد البشرية من يمكنه الإجابة على أسئلتك قبل فعل أي شيء غير قانوني.

القانون الدولي والأمن السيبراني

والمجال القانوني المتعلق بالأمن السيبراني بالغ الحداثة مقارنة بالأمن السيبراني ذاته كما ذكرنا من قبل، معظم الدول لديها بعض القوانين المتعلقة بالأمن السيبراني، والمزيد من القوانين ستأتي في المستقبل.

الأمور الأخلاقية في مجال الأمن السيبراني

بالإضافة إلى العمل ضمن السياقات القانونية، ينبغي على محترفي الأمن السيبراني إظهار السلوكيات الأخلاقية.

الأمور الأخلاقية الشخصية

قد يتصرف الأشخاص بشكل غير أخلاقي ولا يخضعون للمحاكمة أو الغرامة أو السجن. ربما لأن هذا الإجراء لم يكن غير قانوني من الناحية الفنية. ولكن هذا لا يعني أنه سلوك مقبول. فالتأكد من السلوكيات الأخلاقية أمر سهل إلى حد ما. ولا يمكن إدراج جميع السلوكيات غير الأخلاقية المختلفة التي يمكن أن يقوم بها أي شخص يمتلك المهارات المتعلقة بالأمن السيبراني. فيما يلي اثنين فقط. اسأل نفسك:

- هل أرغب في اكتشاف اختراق الأشخاص لجهاز الحاسوب وتغيير صوري في مواقع الشبكات الاجتماعية؟
- هل أرغب في اكتشاف أن أحد فنيي تقنية المعلومات الذين أثق بهم لإصلاح شبكتي، أخبر زملائه بمعلوماتي الشخصية التي حصل عليها أثناء العمل على شبكتي؟

إذا كانت إجابتك على أي من هذه الأسئلة بلا، فلا تقم بفعل هذه الأشياء للآخرين.

الأمور الأخلاقية للشركات

الأخلاق هي قواعد السلوك التي يتم فرضها في بعض الأحيان من قبل القوانين. هناك العديد من مجالات الأمن السيبراني التي لا تتناولها القوانين. هذا يعني أن القيام بأشياء قانونية من الناحية التقنية قد لا يدل على أخلاقيتها. ونظراً لأن العديد من مجالات الأمن السيبراني غير مشمولة بالقوانين (أو لم يتم تضمينها بعد)، فقد أنشأت العديد من المنظمات الاحترافية في مجال تكنولوجيا المعلومات القواعد الأخلاقية للأشخاص داخل هذا المجال. فيما يلي قائمة بثلاثة مؤسسات تطبق القوانين الأخلاقية:

- نشر معهد CyberSecurity (CSI) قوانين أخلاقية يمكن قراءتها هنا.
- وتمتلك منظمة أمن نظم المعلومات (ISSA) مدونة أخلاقيات موجودة هنا.
- وتمتلك رابطة محترفي تقنية المعلومات (AITP) القوانين الأخلاقية ومعايير السلوك الموجودة هنا.

وتمتلك Cisco فريقًا مكرسًا بشكل حصري لسلوكيات الأعمال الأخلاقية. حتى إذا كنت لا تعمل في Cisco ، يمكنك بسهولة تطبيق الأسئلة والأجوبة الموجودة في شجرة القرارات في مكان عملك. وكما هو الحال مع الأسئلة القانونية، بشكل عام، إذا كنت مرتبكًا حول ما إذا كان الإجراء أو السلوك غير أخلاقي، افترض أنه غير أخلاقي ولا تفعله. قد يكون هناك شخص ما في قسم الموارد البشرية أو قسم الشئون القانونية في شركتك يمكنه توضيح موقفك قبل أن تفعل شيئًا يعتبر غير أخلاقي.

ابحث عبر الإنترنت للعثور على المنظمات الأخرى ذات الصلة بتكنولوجيا المعلومات التي تمتلك للقوانين الأخلاقية. حاول أن تجد ما هو مشترك بينها.

وظائف الأمن السيبراني

العديد من الشركات والصناعات الأخرى توظف المتخصصين في الأمن السيبراني. هناك العديد من محركات البحث على الإنترنت لمساعدتك في العثور على الوظيفة المناسبة في مجال الأمن السيبراني:

- ITJobMatch يتخصص محرك البحث ITJobMatch في وظائف تكنولوجيا المعلومات من أي نوع، في جميع أنحاء العالم.
- Monster هو محرك بحث لجميع أنواع الوظائف. ينتقل الرابط مباشرة إلى وظائف الأمن السيبراني.
- CareerBuilder هو محرك بحث لجميع أنواع الوظائف. ينتقل الارتباط مباشرة إلى وظائف الأمن السيبراني.

هذه ليست سوى ثلاثة من العديد من مواقع البحث عن الوظائف المختلفة على الإنترنت. حتى إذا كنت قد بدأت للتو تعليمك في مجال تكنولوجيا المعلومات والأمن السيبراني، فإن الاطلاع على محركات البحث للبحث عن الوظائف هي وسيلة جيدة لمعرفة أنواع الوظائف المتاحة في جميع أنحاء العالم.

وطبقًا لاهتماماتك بالأمن السيبراني، قد تتوفر لك أنواع مختلفة من الوظائف، وقد تتطلب شهادات مهنية متخصصة. على سبيل المثال، يقوم مختبِر الاختراقات، المعروف أيضًا باسم المهاجم الأخلاقي، بالبحث عن نقاط الضعف الأمنية في التطبيقات والشبكات والأنظمة واستغلالها. لكي تصبح مختبرًا للاختراقات، ستحتاج إلى اكتساب الخبرة في وظائف تكنولوجيا المعلومات الأخرى، مثل مسؤول

الأمان ومسؤول الشبكة ومسؤول النظام. تتطلب كل واحدة من هذه الوظائف مجموعتها الخاصة من المهارات التي ستساعدك لكي تصبح ذو قيمة كبيرة للمنظمة.

نأمل أن تكون هذه الدورة قد حمستك على السعي للحصول على تعليم في مجال تكنولوجيا المعلومات والأمن السيبراني ومواصلة المسيرة العملية الرائعة! وتوفر Cisco Networking Academy العديد من الدورات التدريبية لمواصلة التعلم للأمن الإلكتروني. نحن نشجعك على التسجيل في الدورة التدريبية التالية وهي أساسيات الأمن السيبراني، لمواصلة اكتساب المعرفة الأساسية القوية حول الأمن السيبراني. تعرف على Cisco Networking Academy واطلع على قائمة الدورات التدريبية المتاحة. علاوة على ذلك، يمكنك أيضا الوصول إلى الموارد المهنية المتوفرة في Cisco Networking Academy.

وللمتعة انقر هنا لقراءة رواية مصورة عن بطل خارق من أبطال الأمن السيبراني!